aws

Equilibrador de carga de aplicación

# Elastic Load Balancing

# Elastic Load Balancing: Equilibrador de carga de aplicación

# Table of Contents

# ¿Qué es un Equilibrador de carga de aplicación?

Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, como EC2 instancias, contenedores y direcciones IP, en una o más zonas de disponibilidad. Monitorea el estado de los destinos registrados y enruta el tráfico solamente a destinos en buen estado. Elastic Load Balancing escala el equilibrador de carga a medida que el tráfico entrante va cambiando con el tiempo. Puede escalarse automáticamente para adaptarse a la mayoría de las cargas de trabajo.

Elastic Load Balancing admite los siguientes equilibradores de carga: equilibradores de carga de aplicaciones, Equilibradores de carga de red, equilibradores de carga de puerta de enlace y Equilibradores de carga clásicos. Puede seleccionar el tipo de equilibrador de carga que mejor se adapte a sus necesidades. En esta guía, se describen los equilibradores de carga de aplicaciones. Para obtener más información sobre los otros equilibradores de carga, consulte la Guía del usuario sobre Equilibradores de carga de red, la Guía del usuario sobre equilibradores de carga de puerta de enlace y la Guía del usuario sobre Equilibradores de carga clásicos.

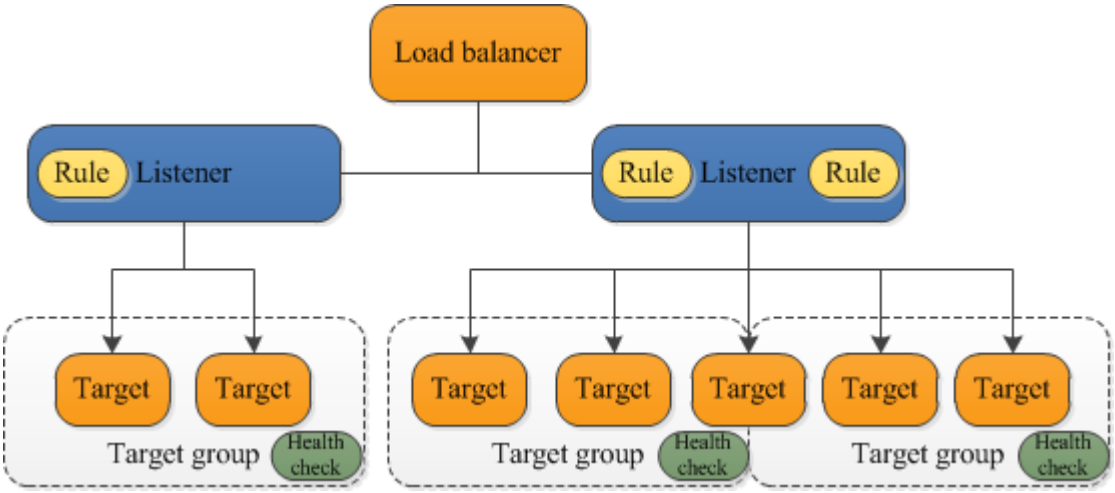
## Componentes del Equilibrador de carga de aplicación

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

Un oyente comprueba las solicitudes de conexión de los clientes mediante el protocolo y el puerto configurados. Las reglas que defina para un oyente determinan cómo el equilibrador de carga va a direccionar las solicitudes a sus destinos registrados. Cada regla consta de una prioridad, una o más acciones y una o más condiciones. Cuando se cumplen las condiciones de una regla, se llevan a cabo sus acciones. Debe definir una regla predeterminada para cada oyente y, si lo desea, puede definir reglas adicionales.

Cada grupo de destino enruta las solicitudes a uno o más destinos registrados, como EC2 instancias, mediante el protocolo y el número de puerto que especifique. 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 oyente del equilibrador de carga.

En el siguiente diagrama se ilustran los componentes básicos. Observe que cada oyente contiene una regla predeterminada y que un oyente 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 siguiente documentación sobre :

- Equilibradores de carga
- Oyentes
- Grupos de destino

# Información general sobre Equilibrador de carga de aplicación

Un Equilibrador de carga de aplicación actúa como la capa de aplicación, es decir, la séptima capa del modelo de interconexión de sistemas abiertos (OSI). Una vez que el equilibrador de carga ha recibido una solicitud, evalúa las reglas del oyente 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 oyente de tal forma que las solicitudes se direccionen a diferentes grupos de destino en función del contenido del tráfico de aplicación. El enrutamiento se lleva a cabo de manera independiente para cada grupo de destino, aunque un destino se haya registrado en varios grupos de destino. Puede configurar el algoritmo de direccionamiento utilizado en el nivel de grupo de destino. El algoritmo de direccionamiento predeterminado es turnos rotativos; alternativamente, puede especificar el algoritmo de direccionamiento de solicitudes menos pendientes.

Puede agregar y eliminar destinos del equilibrador de carga en función de sus necesidades sin interrumpir el flujo general de solicitudes a la aplicación. Elastic Load Balancing escala el equilibrador

de carga a medida que va cambiando el tráfico dirigido a la aplicación con el tiempo. 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 equilibrador de carga solo pueda enviar solicitudes a los destinos en buen estado.

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

## Ventajas de migrar desde un Equilibrador de carga clásico

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

- Compatibilidad con Condiciones de ruta. Puede configurar reglas para el oyente 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 Condiciones de host. Puede configurar reglas para el oyente 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 equilibrador de carga.
- Compatibilidad para direccionamiento basado en campos en la solicitud, como, por ejemplo, Condiciones de los encabezados HTTP y métodos, parámetros de la consulta y direcciones IP de origen.
- Support para el enrutamiento de solicitudes a múltiples aplicaciones en una sola EC2 instancia. Puede registrar cada instancia o dirección IP con múltiples grupos 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 equilibrador de carga.
- Compatibilidad para registrar funciones de Lambda como destinos.
- Compatibilidad para que el equilibrador 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.
- Support para monitorear el estado de cada servicio de forma independiente, ya que los controles de estado se definen a nivel del grupo objetivo y muchas CloudWatch métricas se informan a nivel del grupo objetivo. Si adjunta un grupo de destino a un grupo de escalado automático, podrá escalar cada servicio de forma dinámica en función de la demanda.
- Los registros de acceso contienen información adicional y se almacenan en formato comprimido.
- Mejora del desempeño del equilibrador de carga.

Para obtener más información sobre las funciones compatibles con cada tipo de balanceador de carga, consulta Características de Elastic Load Balancing.

## Servicios relacionados

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

- Amazon EC2: servidores virtuales que ejecutan sus aplicaciones en la nube. Puede configurar su balanceador de carga para enrutar el tráfico a sus EC2 instancias.
- Amazon EC2 Auto Scaling: garantiza que está ejecutando la cantidad de instancias deseada, incluso si una instancia falla, y le permite aumentar o disminuir automáticamente la cantidad de instancias a medida que cambia la demanda de sus instancias. Si habilita el escalado automático con Elastic Load Balancing, las instancias que se lanzan con escalado automático se registran automáticamente en el grupo de destino y las instancias que se terminan con escalado automático se cancelan automáticamente del grupo de destino.
- AWS Certificate Manager: Al crear un oyente HTTPS, puede especificar un certificado específico por ACM. El equilibrador de carga utiliza certificados para terminar las conexiones y descifrar las solicitudes de los clientes. Para obtener más información, consulte Certificados SSL para el Equilibrador de carga de aplicación.
- Amazon CloudWatch: le permite monitorear su balanceador de carga y tomar las medidas necesarias. Para obtener más información, consulte CloudWatch métricas para su Application Load Balancer.
- Amazon ECS: le permite ejecutar, detener y administrar contenedores de Docker en un clúster de EC2 instancias. Puede configurar el equilibrador de carga de forma que direccione el tráfico a los

contenedores. Para obtener más información, consulte Equilibrio de carga de servicio en la Guía para desarrolladores de Amazon Elastic Container Service.

- AWS Global Accelerator: mejora la disponibilidad y el rendimiento de la aplicación. Utilice un acelerador para distribuir el tráfico entre varios balanceadores de carga en una o más regiones. AWS Para obtener más información, consulte la Guía para desarrolladores de AWS Global Accelerator.
- Route 53: proporciona una forma fiable y rentable de dirigir a los visitantes a los sitios web al traducir los nombres de dominio (por ejemplo`www.example.com`) en direcciones IP numéricas (por ejemplo`192.0.2.1`) que utilizan las computadoras para conectarse entre sí. AWS asigna URLs a sus recursos, como los balanceadores de carga. No obstante, puede ser conveniente utilizar una URL que los usuarios puedan recordar fácilmente. Por ejemplo, puede asignar el nombre de dominio a un equilibrador de carga. Para obtener más información, consulte Enrutamiento del tráfico a un equilibrador de carga de ELB en la Guía para desarrolladores de Amazon Route 53.
- AWS WAF— Puede usarlo AWS WAF con su Application Load Balancer para permitir o bloquear las solicitudes en función de las reglas de una lista de control de acceso web (ACL web). Para obtener más información, consulte AWS WAF.

Para ver información sobre los servicios que están integrados en su balanceador de cargas, seleccione su balanceador de cargas en AWS Management Console y elija la pestaña Servicios integrados.

## Precios

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

# Introducción a los equilibradores de carga de aplicaciones

Este tutorial proporciona una introducción práctica a los balanceadores de carga de aplicaciones a través de una interfaz basada en la AWS Management Console web. Para crear el primer Equilibrador de carga de aplicación, siga los pasos que se describen a continuación.

Contenido



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

## Antes de empezar

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

## Paso 1: Configurar un grupo de destino

Cree el grupo de destino que se va a utilizar para el enrutamiento de solicitudes. La regla predeterminada del oyente direcciona las solicitudes a los destinos registrados en este grupo de destino. El equilibrador de carga comprueba el estado de los destinos del grupo utilizando las opciones de comprobación de estado definidas en el grupo de destino.

Para configurar el grupo de destino mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Elija Crear grupo de destino.
4. En Configuración básica, mantenga el tipo de destino como instancia.
5. En Nombre del grupo de destino, ingrese un nombre para el grupo de destino nuevo.
6. Mantenga el protocolo (HTTP) y el puerto (80) predeterminados.
7. Elija la VPC que contiene sus instancias. Mantenga la versión del protocolo como HTTP1.
8. En Health checks (Comprobaciones de estado), mantenga la configuración predeterminada.
9. Elija Next (Siguiente).
10. En la página Registrar destinos, siga los pasos que se describen a continuación. Este es un paso opcional para crear el equilibrador de carga. Sin embargo, debe registrar este destino si quiere probar el equilibrador de carga y asegurarse de que enruta el tráfico a este destino.
    a. En Instancias disponibles, seleccione una o varias instancias.
    b. Mantenga el puerto 80 predeterminado y elija Incluir como pendiente a continuación.
11. Elija Crear grupo de destino.

# Paso 2: Elegir un tipo de equilibrador de carga

Elastic Load Balancing admite distintos tipos de equilibradores de carga. Para este tutorial, debe crear un Equilibrador de carga de aplicación.

Para crear un Equilibrador de carga de aplicación mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, elija una región para el equilibrador de carga. Asegúrese de elegir la misma región que utilizó para sus EC2 instancias.
3. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
4. Elija Crear equilibrador de carga.
5. Para Equilibrador de carga de aplicación (Balanceador de carga de aplicaciones), elija Create (Crear).

# Paso 3: Configurar un equilibrador de carga y un oyente

Para crear un Equilibrador de carga de aplicación, en primer lugar, proporcione alguna información de configuración básica para el equilibrador de carga como, por ejemplo, un nombre, un esquema y un tipo de dirección IP. Luego, proporcione información sobre su red y sobre uno o más oyentes. Un oyente es un proceso que verifica solicitudes de conexión. Se configura con un protocolo y un puerto para las conexiones entre los clientes y el equilibrador de carga. Para obtener más información acerca de los puertos y protocolos compatibles, consulte Configuración del oyente.

Para configurar el equilibrador de carga y el oyente

1. En Load Balancer name (Nombre del equilibrador de carga), escriba un nombre para el equilibrador de carga. Por ejemplo, `my-alb`.
2. Para Scheme y IP address type, mantenga los valores predeterminados.
3. Para el mapeo de redes, selecciona la VPC que usaste para tus EC2 instancias. Seleccione como mínimo dos zonas de disponibilidad y una subred por zona. Para cada zona de disponibilidad que utilizó para lanzar las EC2 instancias, seleccione la zona de disponibilidad y, a continuación, seleccione una subred pública para esa zona de disponibilidad.
4. Para grupos de seguridad, se seleccione el grupo de seguridad predeterminado para la VPC que se eligió en el paso anterior. Puede asociar un grupo de seguridad distinto. El grupo de seguridad debe incluir reglas que permitan que el equilibrador de carga se comunique con los destinos registrados tanto en el puerto del oyente como en el puerto de comprobación de estado. Para obtener más información, consulte Reglas del grupo de seguridad.
5. Para los oyentes y el enrutamiento, mantenga el protocolo y el puerto predeterminados y seleccione su grupo de destino de la lista. Esto configura un oyente que acepta el tráfico HTTP en el puerto 80 y reenvía el tráfico al grupo de destino seleccionado de forma predeterminada. En este tutorial, no va a crear un oyente HTTPS.
6. Como acción predeterminada, seleccione el grupo de destino que creó y registró en el paso 1: Configurar el grupo de destino.
7. (Opcional) Agregue una etiqueta para categorizar su equilibrador de carga. Las claves de las etiquetas deben ser únicas en cada equilibrador de carga. Los caracteres permitidos son letras, espacios y números (en UTF-8), además de los siguientes caracteres especiales: + - =. _ : / @. No utilice espacios iniciales ni finales. Los valores distinguen entre mayúsculas y minúsculas.
8. Revise la configuración y elija Create load balancer (Crear equilibrador de carga). Durante la creación, se aplican algunos atributos predeterminados al equilibrador de carga. Puede verlos

y editarlos después de crear el equilibrador de carga. Para obtener más información, consulte Atributos del equilibrador de carga.

## Paso 4: Probar un equilibrador de carga

Después de crear el balanceador de cargas, verifica que esté enviando tráfico a tus EC2 instancias.

Para probar el equilibrador de carga

1. Una vez que se le notifique que el equilibrador de carga se ha creado correctamente, elija Close.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el grupo de destino que se acaba de crear.
4. Elija Targets y verifique que las instancias estén 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 equilibrador de carga.
5. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
6. Seleccione el equilibrador de carga recién creado.
7. Selecciona Descripción y copia el nombre DNS del balanceador de cargas (por ejemplo, my-load-balancer -1234567890abcdef. elb.us-east-2.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.
8. (Opcional) Para definir reglas de oyente adicionales, consulte Agregar una regla.

## Paso 5: (Opcional) Eliminar el equilibrador de carga

Tan pronto como un equilibrador de carga esté disponible, se le facturará por cada hora u hora parcial que se mantenga en ejecución. Cuando ya no necesite un equilibrador de carga, puede eliminarlo. Tan pronto como se elimine el equilibrador de carga, dejarán de acumularse cargos por él. Tenga en cuenta que, cuando se elimina un equilibrador de carga, los destinos registrados con él no se ven afectados. Por ejemplo, tus EC2 instancias seguirán ejecutándose después de eliminar el balanceador de cargas creado en esta guía.

Para eliminar el equilibrador de carga mediante la consola

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

2. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
3. Seleccione la casilla de verificación para el equilibrador de carga y, a continuación, elija Acciones, Eliminar.
4. Cuando se le indique que confirme, seleccione Yes, Delete (Sí, borrar).

# Introducción a los balanceadores de carga de aplicaciones mediante el AWS CLI

Este tutorial proporciona una introducción práctica a los balanceadores de carga de aplicaciones a través del. AWS CLI

Contenido



## Antes de empezar

- Utilice el siguiente comando para asegurarse de que está ejecutando una versión de la AWS CLI compatible con los equilibradores de carga de aplicaciones.

  ```
  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 última versión de AWS CLI en la Guía del AWS Command Line Interface usuario.
- Lance sus EC2 instancias en una nube privada virtual (VPC). Asegúrese de que los grupos de seguridad de estas instancias permiten obtener acceso al puerto del oyente y al puerto de comprobación de estado. Para obtener más información, consulte Grupos de seguridad de destino.
- Decide si vas a crear un balanceador de cargas IPv4 o uno de doble pila. IPv4 Utilízalo si quieres que los clientes se comuniquen con el balanceador de cargas únicamente mediante direcciones. IPv4 Usa dualstack si quieres que los clientes se comuniquen con el balanceador de cargas mediante direcciones y. IPv4 IPv6 También puedes usar dualstack para comunicarte con los destinos de backend, como IPv6 aplicaciones o subredes de doble pila, utilizando. IPv6

- 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.

## Crear el equilibrador de carga

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

Para crear un equilibrador de carga

1. Usa el create-load-balancercomando para crear un balanceador de cargas. Debe especificar dos subredes que no estén en la misma zona de disponibilidad.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer  \
   --subnets subnet-0e3f5cac72EXAMPLE subnet-081ec835f3EXAMPLE --security-groups
    sg-07e8ffd50fEXAMPLE
   ```

   Usa el create-load-balancercomando para crear un balanceador de **dualstack** cargas.

   ```
   aws elbv2 create-load-balancer --name my-load-balancer  \
   --subnets subnet-0e3f5cac72EXAMPLE subnet-081ec835f3EXAMPLE --security-groups
    sg-07e8ffd50fEXAMPLE --ip-address-type dualstack
   ```

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

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

2. Usa el create-target-groupcomando para crear un grupo objetivo, especificando la misma VPC que usaste para tus EC2 instancias.

   Puedes crear IPv4 y IPv6 segmentar grupos para asociarlos a los balanceadores de carga de doble pila. El tipo de dirección IP del grupo de destino determina la versión de IP que utilizará el equilibrador de carga para comunicarse con tus destinos de backend y comprobar su estado.

   ```
   aws elbv2 create-target-group --name my-targets --protocol HTTP --port 80 \
   --vpc-id vpc-0598c7d356EXAMPLE --ip-address-type [ipv4 or ipv6]
   ```

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-0abcdef1234567890 Id=i-1234567890abcdef0
```

4. Utilice el comando create-oyente para crear un oyente del equilibrador 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 oyente con el siguiente formato:

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

5. (Opcional) Puede verificar el estado de los objetivos registrados para su grupo objetivo mediante este comando: describe-target-health

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

## Adición de un oyente HTTPS

Si tiene un equilibrador de carga con un oyente HTTP, puede agregar un oyente HTTPS tal y como se indica a continuación.

Para agregar un oyente HTTPS a un equilibrador de carga

1. Cree un certificado SSL para usarlo con el equilibrador de carga a través de uno de estos métodos:

- Cree o importe el certificado mediante AWS Certificate Manager (ACM). Para obtener más información, consulte Solicitar un certificado público o Importar certificados en la Guía del AWS Certificate Manager usuario.
- Cargue el certificado mediante AWS Identity and Access Management (IAM). Para obtener más información, consulte Working with Server Certificates (Trabajar con certificados de servidores) en la Guía para el usuario de IAM.

2. Utilice el comando create-oyente para crear el oyente con una regla predeterminada que reenvíe las solicitudes al grupo de destino. Cuando cree un oyente 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 direccionamiento basado en rutas

Si tiene un oyente 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 oyente usando un patrón de ruta

1. Utilice el create-target-groupcomando para crear un grupo objetivo:

```
aws elbv2 create-target-group --name my-targets --protocol HTTP --port 80 \
--vpc-id vpc-0598c7d356EXAMPLE
```

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-0abcdef1234567890 Id=i-1234567890abcdef0
```

3. Utilice el comando create-rule para agregar al oyente 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 equilibrador de carga

Cuando ya no necesite el equilibrador 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
```

# Equilibrador de carga de aplicación

Un equilibrador de carga actúa como único punto de contacto para los clientes. Los clientes envían solicitudes al balanceador de cargas y el balanceador de cargas las envía a los destinos, como EC2 las instancias. Para configurar el equilibrador de carga, debe crear grupos de destino y, a continuación, registrar los destinos en esos grupos. También puede crear oyentes para comprobar la existencia de solicitudes de conexión de los clientes, así como reglas de oyentes para direccionar las solicitudes de los clientes a los destinos de uno o varios grupos de destino.

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

Contenido

# Subredes del equilibrador de carga

Al crear un Equilibrador de carga de aplicación, debe habilitar las zonas que contienen sus destinos. Para habilitar una zona, especifique una subred en ella. Elastic Load Balancing crea un nodo de equilibrador de carga en cada zona que especifique.

Consideraciones

- El equilibrador de carga es más eficaz si se asegura de que cada zona habilitada tenga al menos un destino registrado.
- Si registra los destinos en una zona pero no la habilita, estos destinos registrados no recibirán tráfico del equilibrador de carga.
- Si habilita varias zonas para su equilibrador de carga, estas deben ser del mismo tipo. Por ejemplo, no puede habilitar tanto una zona de disponibilidad como zona local.
- Puede especificar una subred que se haya compartido con usted.

Los equilibradores de carga de aplicaciones admiten los siguientes tipos de subredes.

Tipos de subred

- Subredes de zona de disponibilidad
- Subredes de zona local
- Subredes de Outpost

## Subredes de zona de disponibilidad

Debe seleccionar dos subredes en zonas de disponibilidad como mínimo. Se aplican las siguientes restricciones:

- Cada subred tiene que estar en una zona de disponibilidad diferente.
- Para garantizar que el equilibrador de carga puede adaptarse correctamente, asegúrese de que cada subred de zona de disponibilidad del equilibrador de carga tenga un bloque de CIDR con al menos una máscara de bits `/27` (por ejemplo, `10.0.0.0/27`) y al menos ocho direcciones IP libres por subred. Estas ocho direcciones IP son necesarias para permitir que el equilibrador de carga se escale horizontalmente si es necesario. El equilibrador de carga utiliza estas direcciones IP para establecer conexiones con los destinos. Sin ellas, el Equilibrador de carga de aplicación podría tener dificultades al intentar reemplazar un nodo y provocar que se produjera un error.

Nota: Si una subred de Equilibrador de carga de aplicación se queda sin direcciones IP utilizables al intentar escalar, el Equilibrador de carga de aplicación se ejecutará con una capacidad insuficiente. Durante este tiempo, los nodos antiguos seguirán atendiendo el tráfico, pero el intento de escalado estancado puede provocar errores de hasta cinco veces o tiempos de espera al intentar establecer una conexión.

## Subredes de zona local

Puede especificar una o más subredes de zona local. Las siguientes características no son compatibles:

- Funciones de Lambda como destinos
- Autenticación TLS mutua
- Sesiones persistentes
- AWS WAF integración

## Subredes de Outpost

Puede especificar una única subred de Outpost. Se aplican las siguientes restricciones:

- Debe haber instalado y configurado un Outpost en su centro de datos local. Debe contar con una conexión de red fiable entre el Outpost y la región de AWS . Para obtener más información, consulte la Guía del usuario de AWS Outposts.
- El equilibrador de carga requiere dos instancias `large` en el Outpost para los nodos del equilibrador de carga. Los únicos tipos de instancias compatibles con son los siguientes: El equilibrador de carga se escala según sea necesario y cambia el tamaño de los nodos de un tamaño a la vez (de `large` a `xlarge`, luego de `xlarge` a `2xlarge`, y después de `2xlarge` a `4xlarge`). Después de escalar los nodos al tamaño de instancia más grande, si necesita capacidad adicional, el equilibrador de carga agrega instancias `4xlarge` como nodos del equilibrador de carga. Si no tiene suficiente capacidad de instancias o direcciones IP disponibles para escalar el equilibrador de carga, este informa de un evento al AWS Health Dashboard y el estado del equilibrador de carga es `active_impaired`.
- Puede registrar destinos por ID de instancia o por dirección IP. Si registras objetivos en la AWS región para el puesto avanzado, no se utilizarán.
- Las siguientes características no son compatibles:

- AWS Global Accelerator integración
- Funciones de Lambda como destinos
- Autenticación TLS mutua
- Sesiones persistentes
- Autenticación del usuario
- AWS WAF integración

Se puede implementar un Equilibrador de carga de aplicación en instancias c5/c5d, m5/m5d o r5/r5d en un Outpost. La siguiente tabla muestra el tamaño y el volumen de EBS por tipo de instancia que el equilibrador de carga puede usar en un Outpost:

| Tipo y tamaño de instancia | Volumen EBS (GB) |
|---|---|
| c5/c5d | |
| large | 50 |
| xlarge | 50 |
| 2xlarge | 50 |
| 4xlarge | 100 |
| m5/m5d | |
| large | 50 |
| xlarge | 50 |
| 2xlarge | 100 |
| 4xlarge | 100 |
| r5/r5d | |
| large | 50 |
| xlarge | 100 |

| Tipo y tamaño de instancia | Volumen EBS (GB) |
|---|---|
| 2xlarge | 100 |
| 4xlarge | 100 |

## Grupos de seguridad del equilibrador de carga

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

Las reglas de los grupos de seguridad que están asociados con el equilibrador de carga deben permitir el tráfico en ambas direcciones tanto en el oyente como en los puertos de comprobación de estado. Siempre que se agrega un oyente a un equilibrador 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.

## Estado del equilibrador de carga

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

`provisioning`

El equilibrador de carga se está configurando.

`active`

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

`active_impaired`

El equilibrador de carga enruta el tráfico, pero no tiene los recursos que necesita para escalar.

`failed`

El equilibrador de carga no se han podido configurar.

# Atributos del equilibrador de carga

Para configurar su Equilibrador de carga de aplicación, edite sus atributos. Para obtener más información, consulte Edición de los atributos del equilibrador de carga..

A continuación se indican los atributos del equilibrador de carga:

`access_logs.s3.enabled`

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

`access_logs.s3.bucket`

Nombre del bucket de Amazon S3 para los registros de acceso. Este atributo es obligatorio si están habilitados los registros de acceso. Para obtener más información, consulte Habilitación de registros de acceso.

`access_logs.s3.prefix`

Prefijo de la ubicación en el bucket de Amazon S3.

`client_keep_alive.seconds`

El cliente mantiene un valor keepalive, en segundos. El valor predeterminado es de 3600 segundos.

`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.

`ipv6.deny_all_igw_traffic`

Bloquea el acceso de una puerta de enlace de Internet (IGW) al equilibrador de carga, al evitar el acceso no intencionado a su equilibrador de carga interno a través de una puerta de enlace de Internet. Se ha establecido en `false` para los equilibradores de carga con acceso a Internet y `true` para los equilibradores de carga internos. Este atributo no impide el acceso a Internet que no sea de IGW (por ejemplo, mediante peering, AWS Direct Connect Transit Gateway o). AWS VPN

`routing.http.desync_mitigation_mode`

Determina cómo administra el equilibrador de carga las solicitudes que es posible que representen un riesgo de seguridad para la aplicación. Los valores posibles son `monitor`, `defensive` y `strictest`. El valor predeterminado es `defensive`.

`routing.http.drop_invalid_header_fields.enabled`

Indica si el equilibrador de carga elimina los encabezados HTTP con campos de encabezado que no son no válidos (`true`) o si se redireccionan a los destinos (`false`). El valor predeterminado es `false`. Elastic Load Balancing requiere que los nombres de encabezado HTTP válidos se ajusten a la expresión regular `[-A-Za-z0-9]+`, tal como se describe en el Registro de nombres de campos HTTP. Cada nombre consta de caracteres alfanuméricos o guiones. Seleccione `true` si desea que los encabezados HTTP que no se ajusten a este patrón se eliminen de las solicitudes.

`routing.http.preserve_host_header.enabled`

Indica si el Equilibrador de carga de aplicación debe conservar el encabezado `Host` en la solicitud HTTP y ser enviado al destino sin ningún cambio. Los valores posibles son `true` y `false`. El valor predeterminado es `false`.

`routing.http.x_amzn_tls_version_and_cipher_suite.enabled`

Indica si los dos encabezados (`x-amzn-tls-version` y `x-amzn-tls-cipher-suite`), que contienen información sobre la versión de TLS negociada y el conjunto de cifrado, se agregan a la solicitud del cliente antes de enviarla al destino. El encabezado `x-amzn-tls-version` contiene información acerca de la versión del protocolo TLS negociada con el cliente y el encabezado `x-amzn-tls-cipher-suite` contiene información sobre el conjunto de cifrado negociado con el cliente. Ambos encabezados están en formato OpenSSL. Los valores posibles para el atributo son `true` y `false`. El valor predeterminado es `false`.

`routing.http.xff_client_port.enabled`

Indica si el encabezado `X-Forwarded-For` debe conservar el puerto de origen que el cliente utiliza para conectarse al equilibrador de carga. Los valores posibles son `true` y `false`. El valor predeterminado es `false`.

`routing.http.xff_header_processing.mode`

Permite modificar, conservar o eliminar el encabezado `X-Forwarded-For` en la solicitud HTTP antes de que el Equilibrador de carga de aplicación envíe la solicitud al destino. Los valores posibles son `append`, `preserve` y `remove`. El valor predeterminado es `append`.

- Si el valor es `append`, el Equilibrador de carga de aplicación agrega la dirección IP del cliente (del último salto) al encabezado `X-Forwarded-For` en la solicitud HTTP antes de enviarla a los destinos.
- Si el valor es `preserve`, el Equilibrador de carga de aplicación conserva el encabezado `X-Forwarded-For` en la solicitud HTTP y la envía a los destinos sin ningún cambio.
- Si el valor es `remove`, el Equilibrador de carga de aplicación elimina el encabezado `X-Forwarded-For` en la solicitud HTTP antes de enviarla a los destinos.

`routing.http2.enabled`

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

`waf.fail_open.enabled`

Indica si se debe permitir que un balanceador de cargas AWS WAF habilitado enrute las solicitudes a los destinos si no puede reenviarlas a ellos. AWS WAF Los valores posibles son `true` y `false`. El valor predeterminado es `false`.

> **Note**
>
> El atributo `routing.http.drop_invalid_header_fields.enabled` se introdujo para ofrecer protección contra la desincronización de HTTP. El atributo `routing.http.desync_mitigation_mode` se agregó para proporcionar una protección más completa contra la desincronización de HTTP para sus aplicaciones. No es necesario que utilice ambos atributos y puede elegir cualquiera de ellos, en función de los requisitos de la aplicación.

## Tipo de dirección IP

Puede establecer los tipos de direcciones IP que los clientes pueden utilizar para acceder los equilibradores de carga internos y expuestos a Internet.

Los Equilibradores de carga de aplicación admiten los siguientes tipos de direcciones IP:

**`ipv4`**

Los clientes deben conectarse al balanceador de cargas mediante IPv4 direcciones (por ejemplo, 192.0.2.1).

**`dualstack`**

Los clientes pueden conectarse al balanceador de cargas mediante IPv4 direcciones (por ejemplo, 192.0.2.1) y IPv6 direcciones (por ejemplo, 2001:0 db 8:85 a 3:0:0:8 a2e: 0370:7334).

**`dualstack-without-public-ipv4`**

Los clientes deben conectarse al balanceador de cargas mediante direcciones (por ejemplo, 2001:0 db 8:85 a 3:0:0:8 a2e: 0370:7334). IPv6

Consideraciones

- El equilibrador de carga se comunica con los destinos en función del tipo de dirección IP del grupo de destino.
- Cuando habilita el modo de doble pila para el equilibrador de carga, Elastic Load Balancing proporciona un registro DNS AAAA para el equilibrador de carga. Los clientes que se comunican con el balanceador de cargas mediante direcciones resuelven el registro DNS A. IPv4 Los clientes que se comunican con el balanceador de cargas mediante IPv6 direcciones resuelven el registro DNS AAAA.
- El acceso a los equilibradores de carga internos de doble pila a través de la puerta de enlace de Internet está bloqueado para evitar el acceso no deseado a Internet. Sin embargo, esto no impide el acceso a Internet que no sea de IGW (por ejemplo, mediante peering, AWS Direct Connect Transit Gateway o). AWS VPN
- La autenticación Application Load Balancer solo IPv4 se admite cuando se conecta a un proveedor de identidad (IdP) o a un punto de conexión de Amazon Cognito. Sin una IPv4 dirección pública, el balanceador de cargas no puede completar el proceso de autenticación, lo que provoca errores HTTP 500.

Para obtener más información, consulte Actualización de los tipos de direcciones IP para el Equilibrador de carga de aplicación.

# Grupos de direcciones IP de IPAM

Un conjunto de direcciones IP de IPAM es un conjunto de rangos de direcciones IP contiguos (o CIDRs), dentro del administrador de direcciones IP (IPAM) de Amazon VPC. El uso de grupos de direcciones IP de IPAM con su Application Load Balancer le permite organizar las direcciones de acuerdo con IPv4 sus necesidades de enrutamiento y seguridad. Los grupos de direcciones IP de

IPAM deben crearse primero en IPAM para que Application Load Balancer los pueda usar. Para obtener más información, consulte Incorporar sus direcciones IP a IPAM.

Consideraciones

- Los grupos de direcciones IP de IPAM no son compatibles con los balanceadores de carga internos ni con el Dualstack sin un tipo de dirección IP pública. IPv4
- No puedes eliminar una dirección IP de un conjunto de direcciones IP de IPAM si un balanceador de cargas la usa actualmente.
- Durante la transición a un conjunto de direcciones IP de IPAM diferente, las conexiones existentes finalizan según la duración de conservación del cliente HTTP del balanceador de cargas.
- Los grupos de direcciones IP de IPAM se pueden compartir entre varias cuentas. Para obtener más información, consulte Configurar las opciones de integración para su IPAM

Los grupos de direcciones IP de IPAM le ofrecen la opción de incorporar algunos o todos sus rangos de IPv4 direcciones públicas AWS y usarlos con sus balanceadores de carga de aplicaciones. Con un mejor control de la asignación de direcciones IP, podrá gestionar y aplicar de forma más eficaz las políticas y los controles de seguridad y, al mismo tiempo, beneficiarse de unos costes más bajos. El uso de los grupos de direcciones IP de IPAM con los balanceadores de carga de aplicaciones no conlleva cargos adicionales; sin embargo, puede haber cargos asociados al IPAM en función del nivel que se utilice. Para obtener más información, consulte los precios de Amazon VPC

Su conjunto de direcciones IP de IPAM siempre tiene prioridad al lanzar EC2 instancias y balanceadores de carga de aplicaciones, y cuando sus direcciones IP ya no se utilizan, vuelven a estar disponibles de inmediato. Si no hay más direcciones IP asignables en el conjunto de direcciones IP de IPAM, se asignarán las direcciones IP AWS administradas. AWS las direcciones IP administradas conllevan un coste adicional. Para agregar direcciones IP adicionales, puede agregar nuevos rangos de direcciones IP a un conjunto de direcciones IP de IPAM existente.

## Conexiones del equilibrador de carga

Al procesar una solicitud, el equilibrador de carga mantiene dos conexiones: una con el cliente y otra con un destino. La conexión entre el cliente y el equilibrador de carga también se denomina conexión de front-end. La conexión entre el destino y el equilibrador de carga también se denomina conexión de back-end.

# Equilibrio de carga entre zonas

Con los equilibradores de carga de aplicaciones, el equilibrio de carga entre zonas está activado de forma predeterminada y no se puede cambiar a nivel del equilibrador de carga. Para obtener más información, consulte la sección Equilibrio de carga entre zonas en la Guía del usuario de Elastic Load Balancing.

Es posible desactivar el equilibrio de carga entre zonas a nivel del grupo de destino. Para obtener más información, consulte the section called “Deshabilitar el equilibrio de carga entre zonas”.

# Nombre de DNS

Cada Application Load Balancer recibe un nombre de sistema de nombres de dominio (DNS) predeterminado con la siguiente sintaxis: *name id* -.elb. *region*.amazonaws.com. Por ejemplo, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com.

Si prefiere utilizar un nombre DNS que sea más fácil de recordar, puede crear un nombre de dominio personalizado y asociarlo con el nombre DNS del Equilibrador de carga de aplicación. Cuando un cliente realiza una solicitud mediante este nombre de dominio personalizado, el servidor DNS lo resuelve para hallar el nombre de DNS del Equilibrador de carga de aplicación.

En primer lugar, registre un nombre de dominio con un registrador de nombres de dominio acreditado. A continuación, utilice su servicio de DNS (por ejemplo, su registrador de dominio) para crear un registro de DNS y direccionar las consultas al Equilibrador de carga de aplicación. Para obtener más información, consulte la documentación de su servicio de DNS. Por ejemplo, si utiliza Amazon Route 53 como servicio de DNS, cree un registro de alias que apunte a su Equilibrador de carga de aplicación. Para obtener más información, consulte Enrutamiento del tráfico a un equilibrador de carga de ELB en la Guía para desarrolladores de Amazon Route 53.

El Equilibrador de carga de aplicación tiene una dirección IP por zona de disponibilidad habilitada. Estas son las direcciones IP de los nodos del Equilibrador de carga de aplicación. El nombre DNS del Equilibrador de carga de aplicación se resuelve en estas direcciones. Por ejemplo, suponga que el nombre de dominio personalizado del Equilibrador de carga de aplicación es `example.applicationloadbalancer.com`. Utilice el siguiente comando dig o nslookup para determinar las direcciones IP de los nodos del Equilibrador de carga de aplicación.

Linux o Mac

```
$ dig +short example.applicationloadbalancer.com
```

Windows

```
C:\> nslookup example.applicationloadbalancer.com
```

El Equilibrador de carga de aplicación tiene registros DNS para sus nodos. Puede usar nombres DNS con la siguiente sintaxis para determinar las direcciones IP de los nodos de Application Load Balancer:. *az* *name*- *id* .elb. *region*.amazonaws.com.

Linux o Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

# Creación de un Equilibrador de carga de aplicación

Un equilibrador 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 privada virtual (VPC) con al menos una subred pública en cada una de las zonas que utilizan sus destinos. Para obtener más información, consulte the section called “Subredes del equilibrador de carga”.

Para crear un balanceador de cargas mediante el, consulte. AWS CLIIntroducción a los balanceadores de carga de aplicaciones mediante el AWS CLI

Para crear un equilibrador de carga mediante el AWS Management Console, complete las siguientes tareas.

Tareas

- Paso 1: Configurar un grupo de destino
- Paso 2: Registrar destinos
- Paso 3: Configurar un equilibrador de carga y un oyente
- Paso 4: Probar el equilibrador de carga

# Paso 1: Configurar un grupo de destino

La configuración de un grupo objetivo te permite registrar objetivos, como EC2 instancias. El grupo de destino que configure en este paso se utilizará como grupo de destino en la regla del oyente al configurar el equilibrador de carga. Para obtener más información, consulte Grupos de destino para los equilibradores de carga de aplicaciones.

Para configurar el grupo de destino mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Target Groups.
3. Elija Crear grupo de destino.
4. En la sección Configuración básica, establezca los siguientes parámetros:

    a. En Seleccionar un tipo de destino, seleccione Instancias para especificar los destinos por ID de instancia o Direcciones IP para especificar los destinos por dirección IP. Si el tipo de destino es una función de Lambda, puede habilitar las comprobaciones de estado al seleccionar Habilitar en la sección Comprobaciones de estado.

    b. En Nombre del grupo de destino, escriba el nombre del grupo de destino.

    c. Modifique el Puerto y el Protocolo según sea necesario.

    d. Si el tipo de destino es Instancias o direcciones IP, elija IPv4o IPv6como tipo de dirección IP; de lo contrario, pase al siguiente paso.

    Tenga en cuenta que solo los destinos con el tipo de dirección IP seleccionado se pueden incluir en este grupo de destinos. El tipo de dirección IP no se puede cambiar una vez que se creó el grupo de destino.

    e. Para la VPC, seleccione una nube privada virtual (VPC) con los destinos que desee incluir en su grupo de destino.

    f. Para la versión de protocolo, seleccione HTTP1cuando el protocolo de solicitud sea HTTP/1.1 o HTTP/2; seleccione HTTP2, cuando el protocolo de solicitud sea HTTP/2 o gRPC; y seleccione gRPC, cuando el protocolo de solicitud sea gRPC.

5. En la sección Comprobaciones de estado, mantenga la configuración predeterminada. En Configuración avanzada de la comprobación de estado, elija el puerto de comprobación de estado, el recuento, el tiempo de espera y el intervalo, y especifique los códigos de éxito. Si las comprobaciones de estado superan el recuento de UnhealthyThresholdCount, el equilibrador de carga inhabilita el destino. Cuando las comprobaciones de estado superan el recuento de

HealthyThresholdCount, el equilibrador de carga vuelve a poner el destino en servicio. Para obtener más información, consulte Comprobaciones de estado de los grupos de destinos del Equilibrador de carga de aplicación..

6. (Opcional) Agregue una o varias etiquetas, como se indica a continuación:
   a. Expanda la sección Etiquetas.
   b. Seleccione Agregar etiqueta.
   c. Escriba la clave y el valor de la etiqueta. Los caracteres permitidos son letras, espacios y números (en UTF-8), además de los siguientes caracteres especiales: + - =. _ : / @. No utilice espacios iniciales ni finales. Los valores distinguen entre mayúsculas y minúsculas.
7. Elija Siguiente.

## Paso 2: Registrar destinos

Puede registrar EC2 instancias, direcciones IP o funciones Lambda como destinos en un grupo de destino. Este es un paso opcional para crear un equilibrador de carga. Sin embargo, debe registrar sus destinos para asegurarse de que el equilibrador de carga enrute el tráfico hacia ellos.

1. En la página Registrar destinos, agregue uno o más destinos de la siguiente manera:
   - Si el tipo de destino es Instancias, seleccione una o más instancias, introduzca uno o más puertos y, a continuación, elija Incluir como pendiente debajo.
   - Si el tipo de destino es direcciones IP, haga lo siguiente:
     a. Seleccione una VPC de red de la lista o elija Otras direcciones IP privadas.
     b. Introduzca la dirección IP manualmente o busque la dirección IP mediante los detalles de la instancia. Puede introducir hasta cinco direcciones IP a la vez.
     c. Introduzca los puertos para enrutar el tráfico a las direcciones IP especificadas.
     d. Seleccione Incluir como pendiente debajo.
   - Si el tipo de destino es Lambda, seleccione una función de Lambda o introduzca el ARN de una función de Lambda y, a continuación, seleccione Incluir como pendiente.
2. Elija Crear grupo de destino.

# Paso 3: Configurar un equilibrador de carga y un oyente

Para crear un Equilibrador de carga de aplicación, en primer lugar, proporcione alguna información de configuración básica para el equilibrador de carga como, por ejemplo, un nombre, un esquema y un tipo de dirección IP. Luego, proporcione información sobre su red y sobre uno o más oyentes. Un oyente es un proceso que verifica solicitudes de conexión. Se configura con un protocolo y un puerto para las conexiones entre los clientes y el equilibrador de carga. Para obtener más información acerca de los puertos y protocolos compatibles, consulte Configuración del oyente.

Configuración del equilibrador de carga y el oyente mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Elija Crear equilibrador de carga.
4. En Equilibrador de carga de aplicación, elija Create (Crear).
5. Configuración básica

    a. En Load Balancer name (Nombre del equilibrador de carga), escriba un nombre para el equilibrador de carga. Por ejemplo, **`my-alb`**. El nombre de su Equilibrador de carga de aplicación debe ser único dentro del conjunto de equilibradores de carga de aplicaciones y Equilibradores de carga de red para la región. Los nombres pueden tener un máximo de 32 caracteres y solo pueden contener caracteres alfanuméricos y guiones. No pueden comenzar ni terminar con un guion ni con `internal-`. El nombre de su Equilibrador de carga de aplicación no se puede cambiar una vez creado.

    b. Para Scheme (Esquema), elija ya sea expuesto a internet o interno. Un equilibrador de carga expuesto a Internet direcciona las solicitudes de los clientes a través de Internet hasta los destinos. Un equilibrador de carga interno direcciona las solicitudes hasta los destinos mediante direcciones IP privadas.

    c. Para el tipo de dirección IP IPv4, elija Dualstack o Dualstack without public. IPv4 Elige IPv4si tus clientes usan IPv4 direcciones para comunicarse con el balanceador de cargas. Elige Dualstack si tus clientes usan ambas IPv4 IPv6 direcciones para comunicarse con el balanceador de cargas. Elige Dualstack sin público IPv4 si tus clientes solo usan IPv6 direcciones para comunicarse con el balanceador de cargas.

6. Asignación de redes

a. Para la VPC, selecciona la VPC que usaste para las instancias. EC2 Si ha seleccionado Conexión a Internet para Scheme, solo podrá seleccionarla VPCs con una puerta de enlace a Internet.

b. En el caso de los grupos de direcciones IP de IPAM, puede optar por utilizar el grupo de direcciones IP de IPAM para las direcciones públicas. IPv4 Para obtener más información, consulte Grupos de direcciones IP de IPAM

c. Para las zonas de disponibilidad y las subredes, habilite las zonas para su balanceador de cargas seleccionando las subredes de la siguiente manera:

   - Subredes de dos o más zonas de disponibilidad
   - Subredes de una o más zonas locales
   - Una subred de Outpost

   Para obtener más información, consulte the section called “Subredes del equilibrador de carga”.

   En el caso de los balanceadores de carga internos, las IPv6 direcciones IPv4 y se asignan desde el CIDR de la subred.

   Si habilitaste el modo Dualstack para el balanceador de cargas, selecciona subredes con bloques CIDR y ambos. IPv4 IPv6

7. En Security groups (Grupos de seguridad), seleccione un grupo de seguridad existente o cree uno nuevo.

   El grupo de seguridad del equilibrador de carga debe permitir que este último se comunique con los destinos registrados tanto en el puerto del oyente como en el puerto de comprobación de estado. La consola puede crear automáticamente un grupo de seguridad para el equilibrador de carga con las reglas que permiten esta comunicación. También puede crear un grupo de seguridad y seleccionarlo. Para obtener más información, consulte Reglas recomendadas.

   (Opcional) Para crear un nuevo grupo de seguridad para el equilibrador de carga, elija Create a new security group (Crear un nuevo grupo de seguridad).

8. En Oyentes y enrutamiento, el valor predeterminado es un oyente que acepta tráfico HTTP en el puerto 80. Puede mantener el puerto y el protocolo predeterminados o elegir otros. En Default action (Acción predeterminada), elija el grupo de destino que ha creado. También puede elegir Add oyente (Agregar oyente) para agregar otro oyente (por ejemplo, un oyente HTTPS).

9. (Opcional) Si utiliza un oyente de HTTPS

   Para la política de seguridad, se recomienda utilizar siempre la política de seguridad predefinida más reciente.

   a. Para el SSL/TLS certificado predeterminado, están disponibles las siguientes opciones:

      - Si creó o importó un certificado utilizando AWS Certificate Manager, seleccione Desde ACM y, a continuación, seleccione el certificado en Seleccionar un certificado.
      - Si ha importado un certificado mediante IAM, seleccione Desde IAM y, a continuación, seleccione el certificado en Seleccionar un certificado.
      - Si tiene un certificado para importar pero ACM no está disponible en su región, seleccione Importar y, a continuación, A IAM. Escriba el nombre del certificado en el campo Nombre del certificado. En Clave privada del certificado, copie y pegue el contenido del archivo de clave privada (con codificación PEM). En Cuerpo del certificado, copie y pegue el contenido del archivo de certificado de clave pública (con codificación PEM). En Cadena del certificado, 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.

   b. (Opcional) Para habilitar la autenticación mutua, en Gestión de certificados de cliente, habilite la Autenticación mutua (mTLS).

      Cuando está activado, el modo TLS mutuo predeterminado es de acceso directo.

      Si selecciona Verificar con el almacén de confianza:

      - De forma predeterminada, se rechazan las conexiones con certificados de cliente vencidos. Para cambiar este comportamiento, abra la configuración avanzada de mTLS y, en Caducidad del certificado de cliente, seleccione Permitir certificados de cliente caducados.
      - En Almacén de confianza, seleccione un almacén de confianza existente o elija Nuevo almacén de confianza.
        - Si ha elegido un nuevo almacén de confianza, proporcione un nombre de almacén de confianza, la ubicación de la entidad de certificación URI S3 y, si lo desea, una ubicación en la lista de revocaciones de certificados URI S3.
      - (Opcional) Elija si desea activar la publicidad de los nombres de asunto de TrustStore CA.

10. (Opcional) Puede integrar otros servicios con su equilibrador de carga durante la creación, en Optimizar con integraciones de servicios.

    - Tiene la opción de incluir protecciones de seguridad AWS WAF para su equilibrador de carga, con una ACL web existente o que haya creado automáticamente. Tras la creación, la web se ACLs puede gestionar en la AWS WAF consola. Para obtener más información, consulte Asociar o desasociar una ACL web a un AWS recurso en la AWS WAF Guía para desarrolladores.
    - También tiene la opción de hacer que AWS Global Accelerator cree un acelerador y asociar el equilibrador de carga a este. El nombre del acelerador puede tener los siguientes caracteres (hasta 64 caracteres): a-z, A-Z, 0-9, . (punto) y - (guion). Después de crear el acelerador, puede gestionarlo en la consola AWS Global Accelerator. Para obtener más información, consulte Add an accelerator when you create a load balancer en la Guía para desarrolladores de AWS Global Accelerator .

11. Etiquetar y crear

    a. (Opcional) Agregue una etiqueta para clasificar el equilibrador de carga. Las claves de las etiquetas deben ser únicas en cada equilibrador de carga. Los caracteres permitidos son letras, espacios y números (en UTF-8), además de los siguientes caracteres especiales: + - =. _ : / @. No utilice espacios iniciales ni finales. Los valores distinguen entre mayúsculas y minúsculas.

    b. Revise la configuración y elija Create load balancer (Crear equilibrador de carga). Durante la creación, se aplican algunos atributos predeterminados al equilibrador de carga. Puede verlos y editarlos después de crear el equilibrador de carga. Para obtener más información, consulte Atributos del equilibrador de carga.

## Paso 4: Probar el equilibrador de carga

Tras crear el balanceador de cargas, puedes comprobar que tus EC2 instancias pasan la comprobación de estado inicial. A continuación, puedes comprobar que el balanceador de cargas envía tráfico a tu EC2 instancia. Para eliminar el equilibrador de carga, consulte Eliminación de un Equilibrador de carga de aplicación.

Para probar el equilibrador de carga

1. Una vez creado el equilibrador de carga, elija Close (Cerrar).
2. En el panel de navegación, elija Target Groups.

3. Seleccione el grupo de destino que se acaba de crear.
4. Elija Targets y verifique que las instancias estén listas. Si el estado de una instancia es `initial`, normalmente se debe a que la instancia aún está en proceso de registro. Este estado también puede indicar que la instancia no ha superado el número mínimo de comprobaciones de estado para considerarse en buen estado. Cuando el estado de al menos una instancia sea healthy, podrá probar el equilibrador de carga. Para obtener más información, consulte Estado del destino.
5. En el panel de navegación, seleccione Equilibradores de carga.
6. Seleccione el equilibrador de carga recién creado.
7. Selecciona Descripción y copia el nombre DNS del balanceador de cargas interno o conectado a Internet (por ejemplo, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com).

   - En el caso de los equilibradores de carga orientados a Interne, pegue el nombre de DNS en el campo de direcciones de un navegador web conectado a la Internet.
   - Para los equilibradores de carga internos, pegue el nombre DNS en el campo de direcciones de un navegador web que tenga conectividad privada con la VPC.

   Si todo está configurado correctamente, el navegador mostrará la página predeterminada del servidor.
8. Si la página web no aparece, consulte los siguientes documentos para obtener ayuda adicional sobre la configuración y los pasos de solución de problemas.

   - Para obtener más información, consulte Enrutamiento del tráfico a un equilibrador de carga ELB en la Guía para desarrolladores de Amazon Route 53.
   - Para problemas relacionados con el equilibrador de carga, consulte Solución de problemas de Equilibrador de carga de aplicación.

# Actualización de las zonas de disponibilidad del Equilibrador de carga de aplicación

Puede habilitar o deshabilitar las zonas de disponibilidad del equilibrador de carga en cualquier momento. Después de habilitar una zona de disponibilidad, el equilibrador de carga comienza a direccionar solicitudes a los destinos registrados contenidos en ella. Los balanceadores de carga de aplicaciones tienen activado el equilibrio de carga entre zonas de forma predeterminada, lo que hace que las solicitudes se enruten a todos los destinos registrados en todas las zonas de disponibilidad.

Cuando el equilibrio de carga entre zonas está desactivado, el equilibrador de carga solo enruta las solicitudes a los destinos de la misma zona de disponibilidad. Para obtener más información, consulte Equilibrio de carga entre zonas. El equilibrador 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 equilibrador de carga, pero este último no direcciona solicitudes a ellos.

Para actualizar las zonas de disponibilidad desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Asignación de redes, seleccione Editar subredes.
5. Para habilitar una zona de disponibilidad, marque su casilla de verificación y seleccione una subred. Si hay solo una subred disponible, se seleccionará por usted.
6. Para cambiar la subred en una zona de disponibilidad habilitada, seleccione una de las demás subredes de la lista.
7. Para deshabilitar una zona de disponibilidad, desmarque su casilla de verificación.
8. Seleccione Save changes (Guardar cambios).

Para actualizar las zonas de disponibilidad mediante el AWS CLI

Utilice el comando set-subnets.

# Grupos de seguridad para el Equilibrador de carga de aplicación

El grupo de seguridad del Equilibrador de carga de aplicación controla el tráfico al que se le permite llegar y dejar el equilibrador de carga. Debe asegurarse de que el equilibrador de carga pueda comunicarse con los destinos registrados en el puerto del oyente y en el puerto de comprobación de estado. Cada vez que agregue un oyente al equilibrador de carga o actualice la comprobación de estado de un grupo de destino que el equilibrador de carga utilice para direccionar solicitudes, debe asegurarse de que los grupos de seguridad asociados a ese equilibrador 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 equilibrador de carga o bien asociarle otros grupos de seguridad. Puede elegir los puertos y los protocolos que desee permitir. Por ejemplo, puede abrir conexiones del

Protocolo de mensajes de control de Internet (ICMP) para que el equilibrador de carga responda a las solicitudes de ping (sin embargo, las solicitudes de ping no se reenvían a ninguna instancia).

## Reglas recomendadas

Se recomiendan las siguientes reglas para un equilibrador de carga expuesto a Internet.

Inbound

| Source | Port Range | Comment |
| --- | --- | --- |
| 0.0.0.0/0 | *listener* | Permitir todo el tráfico entrante en el puerto del oyente del equilibrador de carga |

Outbound

| Destination | Port Range | Comment |
| --- | --- | --- |
| *instance security group* | *instance listener* | Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia |
| *instance security group* | *health check* | Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado |

Se recomiendan las siguientes reglas para un equilibrador de carga interno.

Inbound

| Source | Port Range | Comment |
| --- | --- | --- |
| *VPC CIDR* | *listener* | Permitir el tráfico entrante del CIDR de VPC en el puerto del oyente del equilibrador de carga |

Outbound

| Destination | Port Range | Comment |
| --- | --- | --- |
| *instance security group* | *instance listener* | Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia |
| *instance security group* | *health check* | Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado |

Se recomiendan las siguientes reglas para un Equilibrador de carga de aplicación que se utiliza como destino de un Equilibrador de carga de red.

Inbound

| Source | Port Range | Comment |
| --- | --- | --- |
| *client IP addresses/ CIDR* | *alb listener* | Permite el tráfico entrante del cliente en el puerto del oyente del equilibrador de carga. |
| *VPC CIDR* | *alb listener* | Permita que el tráfico de clientes entrante pase por AWS PrivateLink el puerto de escucha del balanceador de carga |
| *VPC CIDR* | *alb listener* | Permitir el tráfico de estado entrante desde el Equilibrador de carga de red |

Outbound

| Destination | Port Range | Comment |
| --- | --- | --- |
| *instance security group* | *instance listener* | Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia |

| | | |
|---|---|---|
| *instance security group* | *health check* | Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado |

Tenga en cuenta que los grupos de seguridad del Equilibrador de carga de aplicación utilizan el seguimiento de las conexiones para realizar un seguimiento de la información sobre el tráfico procedente del Equilibrador de carga de red. Esto ocurre independientemente de las reglas del grupo de seguridad establecidas para su Equilibrador de carga de aplicación. Para obtener más información sobre el seguimiento de EC2 conexiones de Amazon, consulta el seguimiento de conexiones de grupos de seguridad en la Guía del EC2 usuario de Amazon.

Para garantizar que sus destinos reciban tráfico exclusivamente del equilibrador de carga, limite los grupos de seguridad asociados a los destinos para que acepten únicamente el tráfico del equilibrador de carga. Para ello, configure el grupo de seguridad del equilibrador de carga como el origen en la regla de entrada del grupo de seguridad del destino.

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

## Actualizar los grupos de seguridad asociados

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

Para actualizar los grupos de seguridad desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Seguridad, seleccione Editar.
5. Para asociar un grupo de seguridad al equilibrador de carga, selecciónelo. Para eliminar la asociación de un grupo de seguridad, elija el icono X del grupo de seguridad.
6. Seleccione Save changes (Guardar cambios).

Para actualizar los grupos de seguridad mediante el AWS CLI

Utilice el comando set-security-groups.

# Actualización de los tipos de direcciones IP para el Equilibrador de carga de aplicación

Puede configurar su Application Load Balancer para que los clientes puedan comunicarse con el balanceador de cargas únicamente mediante IPv4 direcciones o utilizando ambas IPv6 direcciones ( IPv4 dualstack). El equilibrador de carga se comunica con los destinos en función del tipo de dirección IP del grupo de destino. Para obtener más información, consulte Tipo de dirección IP.

Requisitos de la pila doble

- Puede establecer el tipo de dirección IP al crear el equilibrador de carga y actualizarlo en cualquier momento.
- La nube privada virtual (VPC) y las subredes que especifiques para el balanceador de cargas deben tener bloques CIDR asociados. IPv6 Para obtener más información, consulta IPv6las direcciones en la Guía del EC2 usuario de Amazon.
- Las tablas de rutas de las subredes del balanceador de carga deben enrutar IPv6 el tráfico.
- Los grupos de seguridad del equilibrador de carga deben permitir el tráfico. IPv6
- La red de ACLs las subredes del balanceador de carga debe permitir el tráfico. IPv6

Para establecer el tipo de dirección IP en la creación

Configure los ajustes como se describe en Cree un equilibrador de carga.

Para actualizar el tipo de dirección IP desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Asignación de redes, elija Editar tipo de dirección IP.
5. Para el tipo de dirección IP, elija IPv4admitir solo IPv4 direcciones, Dualstack para admitir ambas IPv6 direcciones IPv4 y, o Dualstack sin público IPv4 para admitir solo direcciones. IPv6
6. Seleccione Save changes (Guardar cambios).

Para actualizar el tipo de dirección IP mediante AWS CLI

Utilice el comando set-ip-address-type.

# Actualice los grupos de direcciones IP de IPAM para su Application Load Balancer

Los grupos de direcciones IP de IPAM deben crearse primero en IPAM para que Application Load Balancer los pueda usar. Para obtener más información, consulte Incorporar sus direcciones IP a IPAM.

Para configurar los grupos de direcciones IP de IPAM en el momento de la creación

Configure los ajustes como se describe en Cree un equilibrador de carga.

Para actualizar los grupos de direcciones IP de IPAM mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Mapeo de redes, selecciona Editar grupos de IP.
5. En Grupos de IP, active Usar grupo de IPAM para IPv4 direcciones públicas.
6. En Grupo de  IPv4 IPAM público, elige el grupo de IPAM que quieres usar.
7. Seleccione Save changes (Guardar cambios).

Para actualizar los grupos de direcciones IP de IPAM mediante el AWS CLI

Utilice el comando modify-ip-pools.

# Integraciones para su aplicación Load Balancer

Puede optimizar la arquitectura de Application Load Balancer integrándola con varios otros AWS servicios para mejorar el rendimiento, la seguridad y la disponibilidad de la aplicación.

Integraciones de balanceadores de carga

- Controlador de recuperación de aplicaciones de Amazon (ARC)
- Amazon CloudFront + AWS WAF
- AWS Global Accelerator
- AWS Config
- AWS WAF

# Controlador de recuperación de aplicaciones de Amazon (ARC)

Amazon Application Recovery Controller (ARC) le ayuda a prepararse y realizar operaciones de recuperación más rápidas para las aplicaciones en ejecución AWS. El cambio zonal y el cambio automático zonal son características de Amazon Application Recovery Controller (ARC).

Con el cambio zonal, puede desviar el tráfico de una zona de disponibilidad reducida con una sola acción. De esta forma, podrá seguir operando desde otras zonas de disponibilidad en buen estado en una Región de AWS.

Con el cambio automático zonal, usted autoriza AWS a desviar el tráfico de recursos de una aplicación desde una zona de disponibilidad durante los eventos, en su nombre, para reducir el tiempo de recuperación. AWS inicia un cambio automático cuando la supervisión interna indica que se ha producido un deterioro en la zona de disponibilidad que podría afectar a los clientes. Cuando se AWS inicia un cambio automático, el tráfico de aplicaciones hacia los recursos que ha configurado para el cambio automático zonal comienza a alejarse de la zona de disponibilidad.

Al activar un cambio de zona, el equilibrador de carga deja de enviar el tráfico nuevo del recurso a la zona de disponibilidad afectada. ARC crea el cambio de zona de inmediato. Sin embargo, las conexiones existentes y en curso en la zona de disponibilidad también pueden tardar poco en completarse, según el comportamiento del cliente y la reutilización de las conexiones. Según la configuración de DNS y otros factores, las conexiones existentes pueden completarse en solo unos minutos o pueden tardar más. Para obtener más información, consulte Limit the time that clients stay connected to your endpoints en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon (ARC).

Para utilizar las funciones de cambio zonal en los balanceadores de carga de aplicaciones, debe tener el atributo de integración de cambios zonales de ARC establecido en Habilitado.

Antes de habilitar la integración de Amazon Application Recovery Controller (ARC) y empezar a utilizar el cambio zonal, revise lo siguiente:

- Puede comenzar un cambio de zona para un equilibrador de carga específico solo para una zona de disponibilidad única. No puede comenzar un cambio de zona para varias zonas de disponibilidad.
- AWS elimina de forma proactiva las direcciones IP de los balanceadores de carga zonales del DNS cuando varios problemas de infraestructura afectan a los servicios. Compruebe siempre la capacidad actual de la zona de disponibilidad antes de comenzar un cambio de zona. Si sus equilibradores de carga tienen desactivado el equilibrio de carga entre zonas y utiliza un cambio

de zona para eliminar la dirección IP del equilibrador de carga de zona, la zona de disponibilidad afectada por el cambio de zona también pierde la capacidad de destino.

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

## Balanceadores de carga de aplicaciones compatibles con zonas cruzadas

Cuando se inicia un cambio zonal en un Application Load Balancer con el equilibrio de carga entre zonas activado, todo el tráfico dirigido a los destinos se bloquea en la zona de disponibilidad afectada y las direcciones IP zonales se eliminan del DNS.

Ventajas:

- Recuperación más rápida de los fallos de la zona de disponibilidad.
- La capacidad de mover el tráfico a una zona de disponibilidad en buen estado si se detectan errores en una zona de disponibilidad.
- Puede probar la integridad de las aplicaciones simulando e identificando los errores para evitar tiempos de inactividad no planificados.

Anulación administrativa por cambio de zona

Los destinos que pertenezcan a un Application Load Balancer incluirán un nuevo estado`AdministrativeOverride`, que es independiente del `TargetHealth` estado.

Cuando se inicia un cambio zonal para un Application Load Balancer, todos los destinos de la zona de la que se está alejando se consideran anulados administrativamente. El Application Load Balancer dejará de enrutar el tráfico nuevo a los destinos anulados administrativamente; sin embargo, las conexiones existentes permanecerán intactas hasta que se cierren orgánicamente.

Los estados posibles de `AdministrativeOverride` son:

unknown

El estado no se puede propagar debido a un error interno

no_override

No existe ninguna anulación activa en el destino actualmente

zonal_shift_active

El cambio de zona está activo en la zona de disponibilidad de destino

## Amazon CloudFront + AWS WAF

Amazon CloudFront es un servicio web que ayuda a mejorar el rendimiento, la disponibilidad y la seguridad de las aplicaciones que utiliza AWS. CloudFront actúa como un punto de entrada único y distribuido para sus aplicaciones web que utilizan balanceadores de carga de aplicaciones. Amplía el alcance de su balanceador de carga de aplicaciones a nivel mundial, lo que le permite atender a los usuarios de manera eficiente desde ubicaciones periféricas cercanas, optimizando la entrega de contenido y reduciendo la latencia para los usuarios de todo el mundo. El almacenamiento automático del contenido en estas ubicaciones periféricas reduce significativamente la carga de su Application Load Balancer, lo que mejora su rendimiento y escalabilidad.

La integración con un solo clic disponible en la consola de Elastic Load Balancing crea una CloudFront distribución con las protecciones de AWS WAF seguridad recomendadas y la asocia a su Application Load Balancer. Las AWS WAF protecciones bloquean los ataques web más comunes antes de que lleguen al balanceador de carga. Puedes acceder a la CloudFront distribución y a su panel de seguridad correspondiente desde la pestaña Integraciones del balanceador de cargas de la consola. Para obtener más información, consulte Administrar las protecciones de AWS WAF seguridad en el panel de CloudFront seguridad de la Guía para CloudFront desarrolladores de Amazon y Introducción a CloudFront Security Dashboard, una CDN unificada y una experiencia de seguridad en aws.amazon.com/blogs.

Como práctica recomendada de seguridad, configure los grupos de seguridad de su balanceador de carga de aplicaciones con conexión a Internet para permitir el tráfico entrante únicamente desde la lista de prefijos AWS gestionada y elimine cualquier otra regla de entrada. CloudFront Para obtener más información, consulte Utilizar la lista de prefijos CloudFront gestionada, Configurar CloudFront para añadir un encabezado HTTP personalizado a las solicitudes y Configurar un Application Load Balancer para reenviar únicamente las solicitudes que contengan un encabezado específico en la Guía para desarrolladores de CloudFront Amazon >.

> **Note**
>
> CloudFront solo admite certificados ACM en la región us-east-1 de EE. UU. Este (Virginia del Norte). Si su Application Load Balancer tiene un agente de escucha HTTPS configurado con un certificado ACM en una región distinta de us-east-1, tendrá que cambiar la conexión de

CloudFront origen de HTTPS a HTTP o proporcionar un certificado ACM en la región EE.UU. Este (Norte de Virginia) y adjuntarlo a su distribución. CloudFront

## AWS Global Accelerator

Para optimizar la disponibilidad, el rendimiento y la seguridad de las aplicaciones, cree un acelerador para su balanceador de cargas. El acelerador dirige el tráfico de la red AWS global a direcciones IP estáticas que sirven como puntos finales fijos en la región más cercana al cliente. AWS Global Accelerator está protegido por Shield Standard, que minimiza el tiempo de inactividad de las aplicaciones y la latencia de los ataques DDo S.

Para obtener más información, consulta Cómo añadir un acelerador al crear un balanceador de cargas en la AWS Global Accelerator Guía para desarrolladores.

## AWS Config

Para optimizar la supervisión y el cumplimiento de tu balanceador de cargas, configúralo. AWS Config AWS Config proporciona una vista detallada de la configuración de AWS los recursos de su AWS cuenta. Esto incluye cómo se relacionan los recursos entre sí y cómo se configuraron en el pasado para que pueda ver cómo cambian las configuraciones y las relaciones a lo largo del tiempo. AWS Config agiliza las auditorías, el cumplimiento y la solución de problemas.

Para obtener más información, consulte ¿Qué es? AWS Config en la Guía para AWS Config desarrolladores.

## AWS WAF

Puede usarlo AWS WAF con su Application Load Balancer para permitir o bloquear las solicitudes según las reglas de una lista de control de acceso web (ACL web).

De forma predeterminada, si el balanceador de cargas no puede obtener una respuesta AWS WAF, devuelve un error HTTP 500 y no reenvía la solicitud. Si necesitas que el balanceador de cargas reenvíe las solicitudes a los destinos aunque no pueda contactar con ellos AWS WAF, puedes habilitar la apertura por AWS WAF error.

Web predefinida ACLs

Al habilitar AWS WAF la integración, puede optar por crear automáticamente una nueva ACL web con reglas predefinidas. La ACL web predefinida incluye tres reglas AWS administradas que ofrecen protección contra las amenazas de seguridad más comunes.

- `AWSManagedRulesAmazonIpReputationList`: el grupo de reglas de la lista de reputaciones de IP de Amazon bloquea las direcciones IP que suelen estar asociadas a bots u otras amenazas. Para obtener más información, consulte Amazon IP reputation list managed rule group en la Guía para desarrolladores de AWS WAF .
- `AWSManagedRulesCommonRuleSet`: el conjunto de reglas básicas (CRS) ofrece protección contra la explotación de una amplia gama de vulnerabilidades, incluyendo algunas de las vulnerabilidades de alto riesgo y más comunes descritas en publicaciones de OWASP tales como OWASP Top 10. Para obtener más información, consulte Grupo de reglas administradas del conjunto de reglas básicas (CRS) en la Guía para desarrolladores de AWS WAF .
- `AWSManagedRulesKnownBadInputsRuleSet`: el grupo de reglas de entradas incorrectas conocidas bloquea los patrones de solicitud que se conocen por no ser válidos y que están asociados a la explotación o el descubrimiento de vulnerabilidades. Para obtener más información, consulte Grupo de reglas administradas de entradas incorrectas conocidas en la Guía para desarrolladores de AWS WAF .

Para obtener más información, consulte Uso de web ACLs in AWS WAF en la Guía para AWS WAF desarrolladores.

# Edición de los atributos del Equilibrador de carga de aplicación

Después de crear un Equilibrador de carga de aplicación, puede editar sus atributos.

Atributos del equilibrador de carga

- Tiempo de inactividad de conexión
- Duración del valor keepalive del cliente HTTP
- Protección contra eliminación
- Modo de mitigación de desincronización
- Conservación del encabezado del host

# Tiempo de inactividad de conexión

El tiempo de espera de la conexión inactiva es el período de tiempo que una conexión de cliente o de destino existente puede permanecer inactiva, sin que se envíen ni reciban datos, antes de que el equilibrador de carga cierre la conexión.

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. También recomendamos que configure el tiempo de inactividad de su aplicación para que sea mayor que el tiempo de inactividad configurado para el equilibrador de carga. De lo contrario, si la aplicación cierra la conexión TCP al equilibrador de carga de forma irregular, este podría enviar una solicitud a la aplicación antes de que reciba el paquete que indica que la conexión está cerrada. Si este es el caso, entonces el equilibrador de carga envía un error HTTP 502 Bad Gateway al cliente.

Los balanceadores de carga de aplicaciones no admiten tramas PING HTTP/2. Estos no restablecen el tiempo de inactividad de la conexión.

De forma predeterminada, Elastic Load Balancing establece el valor del tiempo de inactividad del equilibrador de carga en 60 segundos o 1 minuto. Utilice el procedimiento siguiente para cambiar el valor de tiempo de espera de inactividad.

Actualización el valor del tiempo de espera de la conexión inactiva mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración de tráfico, introduzca un valor en Tiempo de espera de la conexión inactiva, en segundos. El intervalo válido es de 1 a 4000 segundos.
6. Seleccione Save changes (Guardar cambios).

Para actualizar el valor del tiempo de espera de inactividad mediante el AWS CLI

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

# Duración del valor keepalive del cliente HTTP

La duración del valor keepalive del cliente HTTP es el tiempo máximo durante el que un Equilibrador de carga de aplicación mantiene una conexión HTTP persistente con un cliente. Una vez transcurrido el tiempo del valor keepalive del cliente HTTP configurado, el Equilibrador de carga de aplicación acepta una solicitud más y, a continuación, devuelve una respuesta que cierra la conexión sin problemas.

El tipo de respuesta que envía el equilibrador de carga depende de la versión HTTP que usa la conexión del cliente.

- En el caso de los clientes conectados mediante HTTP 1.x, el equilibrador de carga envía un encabezado HTTP que contiene el campo `Connection: close`.
- Para los clientes conectados mediante HTTP/2, el equilibrador de carga envía un marco `GOAWAY`.

De forma predeterminada, Equilibrador de carga de aplicación establece el valor de duración keepalive del cliente HTTP de los equilibradores de carga en 3600 segundos o 1 hora. La duración del valor keepalive del cliente HTTP no se puede desactivar ni establecer por debajo del mínimo de 60 segundos, pero puede aumentarla hasta un máximo de 604 800 segundos o 7 días. Un Equilibrador de carga de aplicación inicia el período de duración del valor keepalive del cliente HTTP cuando se establece inicialmente una conexión HTTP con un cliente. El período de duración continúa cuando no hay tráfico y no se restablece hasta que se confirma una nueva conexión.

Cuando el tráfico del equilibrador de carga se aleja de una zona de disponibilidad dañada mediante un cambio de zona o un cambio automático de zona, los clientes con conexiones abiertas existentes pueden seguir realizando solicitudes a la ubicación afectada hasta que los clientes se vuelvan a conectar. Para conseguir una recuperación más rápida, considere la posibilidad de establecer un valor de duración de keepalive más bajo para limitar el tiempo que los clientes permanecen conectados a un equilibrador de carga. Para obtener más información, consulte Limit the time that clients stay connected to your endpoints en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon (ARC).

> **Note**
>
> Cuando el equilibrador de carga cambia el tipo de dirección IP de su Equilibrador de carga de aplicación a `dualstack-without-public-ipv4`, espera a que se completen todas las conexiones activas. Para reducir el tiempo que se tarda en cambiar el tipo de dirección IP

de su Application Load Balancer, considere reducir la duración del mantenimiento del cliente HTTP.

El Equilibrador de carga de aplicación asigna al cliente HTTP el valor de duración keepalive durante la conexión inicial. Al actualizar la duración del valor keepalive del cliente HTTP, esto puede crear conexiones simultáneas con valores de duración keepalive diferentes del cliente HTTP. Las conexiones existentes conservan el valor de duración keepalive del cliente HTTP que se aplicó durante su conexión inicial. Las nuevas conexiones reciben el valor de duración keepalive del cliente HTTP actualizado.

Actualización del valor de duración keepalive mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración del tráfico, introduzca un valor para la duración del valor keepalive del cliente HTTP. El intervalo válido es de 60 a 604 800 segundos.
6. Seleccione Save changes (Guardar cambios).

Para actualizar el valor de duración del cliente, KeepAlive utiliza el AWS CLI

Utilice el comando modify-load-balancer-attributes con el atributo `client_keep_alive.seconds`.

## Protección contra eliminación

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

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

Para habilitar la protección contra eliminación desde la consola

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

3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración, active Protección contra eliminación.
6. Seleccione Save changes (Guardar cambios).

Para deshabilitar la protección contra eliminación desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Configuración, desactive la Protección contra eliminación.
6. Seleccione Save changes (Guardar cambios).

Para activar o desactivar la protección contra la eliminación mediante el AWS CLI

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

## Modo de mitigación de desincronización

El modo de mitigación de desincronización protege a la aplicación de problemas causados por desincronización HTTP. El equilibrador de carga clasifica cada solicitud en función de su nivel de amenaza, permite solicitudes seguras y, además, mitiga el riesgo según lo especificado en el modo de mitigación que determine. La mitigación de desincronización incluye modos monitoreados, defensivos y más estrictos. El valor predeterminado es el modo defensivo, que proporciona una mitigación duradera contra la desincronización HTTP mientras mantiene la disponibilidad de la aplicación. Puede cambiar al modo más estricto para asegurarse de que la aplicación solo reciba solicitudes que cumplan con RFC 7230.

La biblioteca http_desync_guardian analiza las solicitudes HTTP para evitar ataques de desincronización HTTP. Para obtener más información, consulte HTTP Desync Guardian en. GitHub

Clasificaciones

Las clasificaciones son las siguientes:

- Conforme: la solicitud cumple con RFC 7230 y no presenta amenazas de seguridad conocidas.
- Aceptable: la solicitud no cumple con RFC 7230, pero no presenta amenazas de seguridad conocidas.
- Ambigua: la solicitud no cumple con RFC 7230 y representa un riesgo, ya que varios servidores web y proxies podrían manejarla de manera diferente.
- Grave: la solicitud supone un alto riesgo para la seguridad. El equilibrador de carga bloquea la solicitud, proporciona una respuesta 400 al cliente y cierra la conexión del cliente.

Si una solicitud no cumple con RFC 7230, el equilibrador de carga incrementa la métrica de `DesyncMitigationMode_NonCompliant_Request_Count`. Para obtener más información, consulte Métricas del Equilibrador de carga de aplicación.

La clasificación de cada solicitud se incluye en los registros de acceso al equilibrador de carga. Si la solicitud no cumple con los requisitos, los registros de acceso incluyen un código de motivo de clasificación. Para obtener más información, consulte Motivos de la clasificación.

Modos

En la siguiente tabla se describe cómo los Equilibradores de carga de aplicación tratan a las solicitudes según el modo y la clasificación.

| Clasificación | Modo monitoreado | Modo defensivo | Modo más estricto |
|---|---|---|---|
| Conforme | Permitido | Permitida | Permitida |
| Aceptable | Permitido | Permitida | Bloqueada |
| Ambigua | Permitido | Permitida[1] | Bloqueada |
| Grave | Permitido | Bloqueada | Bloqueada |

[1] Enruta las solicitudes, pero cierra las conexiones del cliente y del destino. Puede incurrir en cargos adicionales si el equilibrador de carga recibe una gran cantidad de solicitudes ambiguas en el modo Defensivo. Esto se debe a que el aumento del número de conexiones nuevas por segundo contribuye a las unidades de capacidad del equilibrador de carga (LCU) utilizadas por hora. Puede usar la métrica `NewConnectionCount` para comparar la forma en que el equilibrador de carga establece nuevas conexiones en el modo Monitor y en el modo Defensivo.

Para actualizar el modo de mitigación de desincronización mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.
5. En Gestión de paquetes, para Modo de mitigación de desincronización, seleccione Defensivo, Más estricto o Monitor.
6. Seleccione Save changes (Guardar cambios).

Para actualizar el modo de mitigación desincronizado mediante el AWS CLI

Utilice el modify-load-balancer-attributescomando con el `routing.http.desync_mitigation_mode` atributo establecido en `monitordefensive`, o. `strictest`

## Conservación del encabezado del host

Cuando habilita el atributo Conservar encabezado de host, el Equilibrador de carga de aplicación conserva el encabezado `Host` de la solicitud HTTP y la envía a los destinos sin ninguna modificación. Si el Equilibrador de carga de aplicación recibe varios encabezados `Host`, los conserva todos. Las reglas de oyente se aplican solo al primer encabezado `Host` recibido.

De forma predeterminada, cuando el atributo Conservar el encabezado del host no está habilitado, el Equilibrador de carga de aplicación modifica el encabezado `Host` de la siguiente manera:

Cuando la conservación del encabezado del host no está habilitada y el puerto de oyente no es un puerto predeterminado: cuando no se utilizan los puertos predeterminados (puertos 80 o 443), agregamos el número de puerto al encabezado del host si el cliente aún no lo ha hecho. Por ejemplo, el encabezado `Host` de la solicitud HTTP con `Host: www.example.com` se modificaría en `Host: www.example.com:8080` si el puerto de oyente no es un puerto predeterminado como `8080`.

Cuando la conservación del encabezado del host no está habilitada y el puerto de oyente es el puerto predeterminado (puerto 80 o 443): en el caso de los puertos de oyente predeterminados (puerto 80 o 443), no agregamos el número de puerto al encabezado del host saliente. Se elimina cualquier número de puerto que ya estuviera en el encabezado del host entrante.

La siguiente tabla muestra más ejemplos de cómo los equilibradores de carga de aplicaciones tratan los encabezados de host en la solicitud HTTP en función del puerto de oyente.

| Puerto del oyente | Ejemplo de solicitud | Encabezado de host en la solicitud | La conservación del encabezado del host está deshabilitada (comportamiento predeterminado) | La conservación del encabezado del host está habilitada |
|---|---|---|---|---|
| La solicitud se envía al HTTP/HTTPS oyente predeterminado. | `GET /index.html HTTP/1.1 Host: example.com` | example.com | example.com | example.com |
| La solicitud se envía en el oyente HTTP predeterminado y el encabezado del host tiene un puerto (por ejemplo, 80 o 443). | `GET /index.html HTTP/1.1 Host: example.com:80` | example.com:80 | example.com | example.com:80 |
| La solicitud tiene una ruta absoluta. | `GET https://dns_name/index.html HTTP/1.1 Host: example.com` | example.com | dns_name | example.com |
| La solicitud se envía a un puerto de oyente no predeterm | `GET /index.html HTTP/1.1` | example.com | example.com:8080 | example.com |

| Puerto del oyente | Ejemplo de solicitud | Encabezado de host en la solicitud | La conservación del encabezado del host está deshabilitada (comportamiento predeterminado) | La conservación del encabezado del host está habilitada |
|---|---|---|---|---|
| inado (por ejemplo, 8080). | `Host: example.com` | | | |
| La solicitud se envía a un puerto de oyente no predeterminado y el encabezado del host tiene un puerto (por ejemplo, 8080). | `GET / index.html HTTP/1.1 Host: example.com:8080` | example.com:8080 | example.com:8080 | example.com:8080 |

Habilitación de la conservación del encabezado del host mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.
5. En Gestión de paquetes, active Conservar el encabezado del host.
6. Seleccione Save changes (Guardar cambios).

Para permitir la conservación del encabezado del host mediante el AWS CLI

Utilice el modify-load-balancer-attributescomando con el `routing.http.preserve_host_header.enabled` atributo establecido en`true`.

# Etiquetado de un Equilibrador de carga de aplicación

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

Puede agregar varias etiquetas a cada equilibrador de carga. Si agrega una etiqueta con una clave que ya está asociada al equilibrador de carga, se actualizará el valor de esa etiqueta.

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

Restricciones

- Número máximo 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 iniciales ni finales.
- No utilice el `aws:` prefijo en los nombres o valores de las etiquetas porque está reservado para su AWS uso. Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar ni eliminar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.

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

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Etiquetas, elija Adminsitrar etiquetas y, a continuación, realice una o varias de las acciones siguientes:
   a. Para actualizar una etiqueta, modifique los valores Key y Value.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, seleccione el botón Remove (Eliminar) junto a la etiqueta.
5. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de un balanceador de carga mediante el AWS CLI

Utilice los comandos add-tags y remove-tags.

# Eliminación de un Equilibrador de carga de aplicación

Tan pronto como un equilibrador de carga esté disponible, se le facturará por cada hora u hora parcial que se mantenga en ejecución. Cuando ya no necesite el equilibrador de carga, puede eliminarlo. Tan pronto como se elimine el equilibrador de carga, dejarán de acumularse cargos por él.

No se puede eliminar un equilibrador de carga si está habilitada la protección contra eliminación. Para obtener más información, consulte Protección contra eliminación.

Tenga en cuenta que eliminar un equilibrador de carga no afecta a los destinos registrados en él. Por ejemplo, tus EC2 instancias siguen ejecutándose y siguen registradas en sus grupos de destino. Para eliminar los grupos de destino, consulte Eliminación de un grupo de destino del Equilibrador de carga de aplicación.

Para eliminar un equilibrador de carga desde la consola

1. Si cuenta con un registro de DNS para el dominio que señala al equilibrador de carga, apúntelo hacia una ubicación nueva y espere a que surta efecto el cambio de DNS antes de eliminar el equilibrador de carga.

   Ejemplo:

   - Si el registro es un registro CNAME con un tiempo de vida (TTL) de 300 segundos, espere al menos 300 segundos antes de continuar con el siguiente paso.
   - Si el registro es un registro Alias (A) de Route 53, espere al menos 60 segundos.
   - Si utiliza Route 53, el cambio de registro tarda 60 segundos en propagarse a todos los servidores de nombres de Route 53 globales. Agregue este tiempo al valor de TTL del registro que se está actualizando.
2. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
3. En el panel de navegación, seleccione Load Balancers.
4. Seleccione el equilibrador de carga y, a continuación, elija Aciones, Eliminar equilibrador de carga.
5. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para eliminar un balanceador de carga mediante el AWS CLI

Utilice el comando delete-load-balancer.

# Visualización del mapa de recursos del Equilibrador de carga de aplicación

El mapa de recursos del Equilibrador de carga de aplicación proporciona una visualización interactiva de la arquitectura del equilibrador de carga, incluidos los oyentes, las reglas, los grupos de destinos y los destinos asociados. El mapa de recursos también destaca las relaciones y las rutas de enrutamiento entre todos los recursos, lo que proporciona una representación visual de la configuración del equilibrador de carga.

Visualización del mapa de recursos del Equilibrador de carga de aplicación mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. Seleccione la pestaña Mapa de recursos para ver el mapa de recursos del equilibrador de carga.

## Componentes del mapa de recursos

### Vistas de mapa

Hay dos vistas disponibles en el mapa de recursos del Equilibrador de carga de aplicación: Información general y Mapa de destinos en mal estado. La información general se selecciona de forma predeterminada y muestra todos los recursos del equilibrador de carga. Si selecciona la vista Mapa de destinos en mal estado, solo se mostrarán los destinos en mal estado y los recursos asociados a ellos.

La vista Mapa de destinos en mal estado se puede utilizar para solucionar problemas en destinos que no superen las comprobaciones de estado. Para obtener más información, consulte Solución de problemas de destinos en mal estado mediante el mapa de recursos.

### Grupos de recursos

El mapa de recursos del Equilibrador de carga de aplicación contiene cuatro grupos de recursos, uno para cada tipo de recurso. Los grupos de recursos son Oyentes, Reglas, Grupos de destinos y Destinos.

Mosaicos de recursos

Cada recurso de un grupo tiene su propio mosaico, que muestra detalles sobre ese recurso concreto.

- Si se pasa el cursor por encima del mosaico de un recurso, se destacan las relaciones entre este y otros recursos.
- Si se selecciona el mosaico de un recurso, se destacan las relaciones entre este y otros recursos y se muestran detalles adicionales sobre el recurso en cuestión.
  - condiciones de la regla: las condiciones de cada regla.
  - Resumen de estado de funcionamiento del grupo de destino: número de destinos registrados para cada estado de funcionamiento.
  - estado de funcionamiento del destino: estado y descripción del funcionamiento actual del destino.

> **Note**
>
> Puede desactivar Mostrar detalles del recurso para ocultar los detalles adicionales en el mapa de recursos.

- Cada mosaico de recurso contiene un enlace que, cuando se selecciona, lleva a la página de detalles de ese recurso.
  - Agentes de escucha: seleccione el puerto del protocolo de los oyentes. Por ejemplo, `HTTP:80`
  - Reglas: seleccione la acción de las reglas. Por ejemplo, `Forward to target group`
  - Grupos de destino: seleccione el nombre del grupo de destino. Por ejemplo, `my-target-group`
  - Destino: seleccione el ID de los destinos. Por ejemplo, `i-1234567890abcdef0`

Exportación del mapa de recursos

Al seleccionar Exportar, tiene la opción de exportar la vista actual del mapa de recursos de su Equilibrador de carga de aplicación en formato PDF.

# Reservas de capacidad para su Application Load Balancer

Las reservas de unidades de capacidad (LCU) del balanceador de cargas te permiten reservar una capacidad mínima estática para tu balanceador de cargas. Los balanceadores de carga de aplicaciones se escalan automáticamente para soportar las cargas de trabajo detectadas y satisfacer

las necesidades de capacidad. Cuando se configura la capacidad mínima, el balanceador de carga sigue aumentando o disminuyendo en función del tráfico recibido, pero también evita que la capacidad disminuya por debajo de la capacidad mínima configurada.

Considere la posibilidad de utilizar la reserva de LCU en las siguientes situaciones:

- Tienes previsto celebrar un evento en el que se va a producir un tráfico repentino e inusual, y quieres asegurarte de que tu balanceador de carga pueda soportar el aumento repentino de tráfico que se produzca durante el evento.
- Tienes picos de tráfico impredecibles debido a la naturaleza de tu carga de trabajo durante un período breve.
- Estás configurando tu balanceador de carga para incorporar o migrar tus servicios a una hora de inicio específica y necesitas empezar con una gran capacidad en lugar de esperar a que el autoscaling surta efecto.
- Debe mantener una capacidad mínima para cumplir con los acuerdos de nivel de servicio o los requisitos de conformidad.
- Está migrando cargas de trabajo entre balanceadores de carga y desea configurar el destino para que coincida con la escala del origen.

### Calcule la capacidad que necesita

A la hora de determinar la cantidad de capacidad que debes reservar para tu balanceador de cargas, te recomendamos realizar pruebas de carga o revisar los datos históricos de carga de trabajo que representan el tráfico próximo que esperas. Con la consola Elastic Load Balancing, puede estimar la capacidad que necesita reservar en función del tráfico revisado.

Como alternativa, puede utilizar la CloudWatch métrica `PeakLCUs` para determinar el nivel de capacidad necesario. La `PeakLCUs` métrica tiene en cuenta los picos de tu patrón de tráfico que el balanceador de cargas debe escalar en todas las dimensiones de escalado para soportar tu carga de trabajo. La `PeakLCUs` métrica es diferente de la `ConsumedLCUs` métrica, que solo agrega las dimensiones de facturación de tu tráfico. Se recomienda usar la `PeakLCUs` métrica para garantizar que la reserva de la LCU sea adecuada durante el escalado del balanceador de carga. A la hora de estimar la capacidad, utiliza un valor por minuto de. `Sum` `PeakLCUs`

Si no tiene datos históricos de carga de trabajo como referencia y no puede realizar pruebas de carga, puede estimar la capacidad necesaria mediante la calculadora de reservas de la LCU. La calculadora de reservas de la LCU utiliza datos basados en el historial de cargas de trabajo,

AWS observe y es posible que no represente su carga de trabajo específica. Para obtener más información, consulta la Calculadora de reservas de unidades de capacidad del Load Balancer.

Cuotas para reservas de LCU

Su cuenta tiene cuotas relacionadas con. LCUs Para obtener más información, consulte the section called “Unidades de capacidad del Load Balancer”.

## Solicita una reserva de unidad de capacidad del balanceador de cargas para tu Application Load Balancer

Antes de utilizar la reserva de la LCU, revise lo siguiente:

- La capacidad está reservada a nivel regional y se distribuye uniformemente entre las zonas de disponibilidad. Confirma que tienes suficientes objetivos distribuidos de manera uniforme en cada zona de disponibilidad antes de activar la reserva de LCU.
- Las solicitudes de reserva en las LCU se tramitan por orden de llegada y dependen de la capacidad disponible en la zona en ese momento. Por lo general, la mayoría de las solicitudes se tramitan en unos minutos, pero pueden tardar hasta unas horas.
- Para actualizar una reserva existente, la solicitud anterior debe estar aprovisionada o haber fallado. Puede aumentar la capacidad reservada tantas veces como necesite, pero solo puede reducirla dos veces al día.
- Seguirá incurriendo en cargos por cualquier capacidad reservada o aprovisionada hasta que se cancele o cancele.

Solicite una reserva de LCU

En los pasos de este procedimiento se explica cómo solicitar una reserva de LCU en el balanceador de carga.

Para solicitar una reserva de LCU mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el nombre del equilibrador de carga.
4. En la pestaña Capacidad, selecciona Editar reserva de LCU.

5. Selecciona Estimación basada en referencias históricas y, a continuación, selecciona el equilibrador de carga en la lista desplegable.
6. Seleccione el período de referencia para ver el nivel de LCU reservado recomendado.
7. Si no tiene una carga de trabajo de referencia histórica, puede elegir Estimación manual e introducir el número LCUs que desea reservar.
8. Seleccione Save.

Para solicitar una reserva en la LCU utilizando AWS CLI

Utilice el comando modify-capacity-reservation.

## Actualice o cancele las reservas de unidades de capacidad del balanceador de cargas para su aplicación Load Balancer

Actualizar o cancelar una reserva de la LCU

En los pasos de este procedimiento se explica cómo actualizar o cancelar una reserva de LCU en el equilibrador de carga.

Para actualizar o cancelar una reserva de LCU mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el nombre del equilibrador de carga.
4. En la pestaña Capacidad, confirma que el estado de la reserva es Aprovisionada.
    a. Para actualizar la reserva de la LCU, seleccione Editar reserva de la LCU.
    b. Para cancelar la reserva de la LCU, seleccione Cancelar capacidad.

Para actualizar o cancelar una reserva de LCU mediante el AWS CLI

Utilice el comando modify-capacity-reservation.

## Supervise la reserva de unidades de capacidad del Load Balancer para su aplicación Load Balancer

Estado de la reserva

La reserva de la LCU tiene cuatro estados disponibles:

- pendiente - Indica la reserva que se encuentra en proceso de aprovisionamiento.
- aprovisionada - Indica que la capacidad reservada está lista y disponible para su uso.
- fallido - Indica que la solicitud no se puede completar en ese momento.
- reequilibrio - Indica que se ha añadido o eliminado una zona de disponibilidad y que el equilibrador de cargas está reequilibrando la capacidad.

### LCU reservada

La `ReservedLCUs` métrica se informa por minuto. La capacidad se reserva cada hora. Por ejemplo, si tiene una reserva en la LCU de 6000 personas, el total de una hora `ReservedLCUs` es de 6000 y el total de un minuto es de 100. Para determinar el uso reservado de la LCU, consulte la métrica. `PeakLCUs` Puede configurar CloudWatch alarmas para comparar el valor por minuto con el valor `Sum` de `PeakLCUs` la capacidad reservada, o el valor por hora `SumReservedLCUs`, para determinar si ha reservado suficiente capacidad para satisfacer sus necesidades.

### Supervise la capacidad reservada

En los pasos de este proceso se explica cómo comprobar el estado de una reserva de LCU en el balanceador de carga.

Para ver el estado de una reserva de LCU mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el nombre del equilibrador de carga.
4. En la pestaña Capacidad, puedes ver el estado de la reserva y el valor de la LCU reservada.

Para supervisar el estado de la reserva de la LCU mediante AWS CLI

Utilice el comando describe-capacity-reservation.

# Oyentes para Equilibrador de carga de aplicación

Un oyente es un proceso que comprueba las solicitudes de conexión utilizando el protocolo y el puerto configurados. Antes de comenzar a utilizar el Equilibrador de carga de aplicación, debe agregar al menos un oyente. Si su equilibrador de carga no cuenta con oyentes, no puede recibir tráfico de los clientes. Las reglas que definas para tus oyentes determinan cómo el balanceador de cargas dirige las solicitudes a los destinos que registras, como EC2 las instancias.

Contenido



## Configuración del oyente

Los oyentes son compatibles con los siguientes protocolos y puertos:

- Protocolos: HTTP, HTTPS
- Puertos: 1-65535

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

Si debe asegurarse de que los destinos descifren el tráfico HTTPS en lugar del equilibrador de carga, puede crear un Equilibrador de carga de red con un oyente TCP en el puerto 443. Con un oyente TCP, el equilibrador de carga transfiere el tráfico cifrado a los destinos sin descifrarlo. Para obtener más información, consulte la Guía del usuario de Equilibradores de carga de red.

WebSockets

Los balanceadores de carga de aplicaciones ofrecen soporte nativo para. WebSockets Puede convertir una conexión HTTP/1.1 existente en una WebSocket (`wsowss`) conexión mediante una actualización de la conexión HTTP. Al actualizar, la conexión TCP utilizada para las solicitudes (tanto al balanceador de carga como al destino) se convierte en una WebSocket conexión persistente entre el cliente y el destino a través del balanceador de cargas. Puedes utilizarla WebSockets con dispositivos de escucha HTTP y HTTPS. Las opciones que elija para su agente de escucha se aplican tanto a WebSocket las conexiones como al tráfico HTTP. Para obtener más información, consulta Cómo funciona el WebSocket protocolo en la Guía para CloudFront desarrolladores de Amazon.

HTTP/2

Los equilibradores de carga de apliación proporcionan soporte nativo para HTTP/2 con oyentes HTTPS. Puede enviar hasta 128 solicitudes a la vez con una conexión HTTP/2. Se puede usar la versión del protocolo para enviar la solicitud a los destinos mediante HTTP/2. Para obtener más información, consulte Versión del protocolo. 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 equilibrador de carga. No puede utilizar la característica server-push de HTTP/2.

La autenticación TLS mutua para los balanceadores de carga de aplicaciones admite HTTP/2 en los modos de transferencia y verificación. Para obtener más información, consulte Autenticación mutua con TLS en Equilibrador de carga de aplicación.

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

## Atributos del oyente

Los siguientes son los atributos de escucha de los balanceadores de carga de aplicaciones:

`routing.http.request.x_amzn_mtls_clientcert_serial_number.header_name`

Permite modificar el nombre del encabezado de la solicitud HTTP X-Amzn-Mtls-Clientcert-Serial-Number.

`routing.http.request.x_amzn_mtls_clientcert_issuer.header_name`

Le permite modificar el nombre del encabezado de la solicitud HTTP X-Amzn-Mtls-Clientcert-Issuer.

`routing.http.request.x_amzn_mtls_clientcert_subject.header_name`

Permite modificar el nombre del encabezado de la solicitud HTTP X-Amzn-Mtls-Clientcert-Subject.

`routing.http.request.x_amzn_mtls_clientcert_validity.header_name`

Permite modificar el nombre del encabezado de la solicitud HTTP X-Amzn-Mtls-Clientcert-Validity.

`routing.http.request.x_amzn_mtls_clientcert_leaf.header_name`

Permite modificar el nombre del encabezado de la solicitud HTTP X-Amzn-Mtls-Clientcert-Leaf.

`routing.http.request.x_amzn_mtls_clientcert.header_name`

Le permite modificar el nombre del encabezado de la solicitud HTTP X-Amzn-Mtls-Clientcert.

`routing.http.request.x_amzn_tls_version.header_name`

Permite modificar el nombre del encabezado de la solicitud HTTP de X-Amzn-Tls-Version.

`routing.http.request.x_amzn_tls_cipher_suite.header_name`

Permite modificar el nombre del encabezado de la solicitud HTTP de X-Amzn-Tls-Cipher-Suite.

`routing.http.response.server.enabled`

Le permite permitir o eliminar el encabezado del servidor de respuesta HTTP.

`routing.http.response.strict_transport_security.header_value`

Informa a los navegadores de que solo se debe acceder al sitio mediante HTTPS y que cualquier intento futuro de acceder a él mediante HTTP debe convertirse automáticamente a HTTPS.

`routing.http.response.access_control_allow_origin.header_value`

Especifica qué orígenes pueden acceder al servidor.

`routing.http.response.access_control_allow_methods.header_value`

Devuelve qué métodos HTTP están permitidos cuando se accede al servidor desde un origen diferente.

`routing.http.response.access_control_allow_headers.header_value`

Especifica qué encabezados se pueden usar durante la solicitud.

`routing.http.response.access_control_allow_credentials.header_value`

Indica si el navegador debe incluir credenciales como cookies o autenticación al realizar las solicitudes.

`routing.http.response.access_control_expose_headers.header_value`

Devuelve qué encabezados puede mostrar el navegador al cliente solicitante.

`routing.http.response.access_control_max_age.header_value`

Especifica durante cuánto tiempo se pueden almacenar en caché los resultados de una solicitud de verificación previa, en segundos.

`routing.http.response.content_security_policy.header_value`

Especifica las restricciones impuestas por el navegador para ayudar a minimizar el riesgo de determinados tipos de amenazas a la seguridad.

`routing.http.response.x_content_type_options.header_value`

Indica si se deben seguir los tipos de MIME anunciados en los encabezados de Content-Type y no se deben cambiar.

`routing.http.response.x_frame_options.header_value`

Indica si el navegador puede representar una página en un marco, iframe, incrustación u objeto.

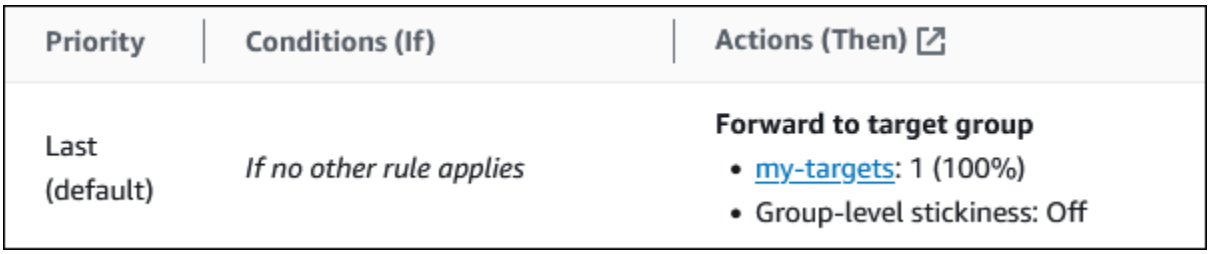
# Reglas del oyente

Cada oyente tiene una acción predeterminada, que se conoce también como regla predeterminada. La regla predeterminada no se puede eliminar y siempre se ejecuta en último lugar. Cada una consta de una prioridad, de una o varias acciones y de una o varias condiciones. Puede agregar y editar reglas en cualquier momento. Para obtener más información, consulte Editar una regla.

## Reglas predeterminadas

Cuando crea un oyente, 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 oyente, 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 reglas 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 Actualizar la prioridad de una regla.

## Acciones de las reglas

Cada acción de regla tiene un tipo, una prioridad y la información necesaria para realizar la acción. Para obtener más información, consulte Tipos de acción de regla.

## 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.

# Tipos de acción de regla

Se admiten los siguientes tipos de acción para una regla de oyente:

`authenticate-cognito`

[Oyentes HTTPS] Utilice Amazon Cognito para autenticar a los usuarios. Para obtener más información, consulte Autenticación de usuarios mediante un Equilibrador de carga de aplicación.

`authenticate-oidc`

[Oyentes HTTPS] Utilice un proveedor de identidades 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.

`forward`

Reenvíe las solicitudes a los grupos de destino especificados. Para obtener más información, consulte Acciones de reenvío.

`redirect`

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

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

Si la versión del protocolo es gRPC o HTTP/2, las únicas acciones admitidas son las acciones de `forward`.

## 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 registros de acceso. El número de acciones `fixed-response` correctas se registra en la métrica `HTTP_Fixed_Response_Count`. Para obtener más información, consulte Métricas del Equilibrador de carga de aplicación.

Example Ejemplo de acción de respuesta fija para el 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 a uno o más grupos de destino. Si especifica varios grupos de destino para una acción `forward`, debe especificar una ponderación para cada grupo de destino. Cada ponderación de grupo de destino es un valor de 0 a 999. Las solicitudes que coinciden con una regla del oyente con los grupos de destino ponderados se distribuyen a estos grupos de destino en función de sus ponderaciones. Por ejemplo, si especifica dos grupos de destino, cada uno con una ponderación de 10, cada grupo de destino recibe la mitad de las solicitudes. Si especifica dos grupos de destino, uno con una ponderación de 10 y el otro con una ponderación de 20, el grupo de destino con una ponderación de 20 recibe el doble de solicitudes que el otro grupo de destino.

Si configuras una regla para distribuir el tráfico entre los grupos objetivo ponderados y uno de los grupos objetivo está vacío o solo tiene destinos en mal estado, el balanceador de cargas no conmuta automáticamente por error a un grupo objetivo con objetivos en buen estado.

De forma predeterminada, la configuración de una regla para distribuir tráfico entre los grupos de destino ponderados no garantiza que se cumplan las sesiones persistente. Para asegurarse de que se respetan las sesiones persistente, habilite la persistencia del grupo de destino para la regla. Cuando el balanceador de cargas dirige por primera vez una solicitud a un grupo objetivo ponderado, genera una cookie cuyo nombre AWSALBTG codifica la información sobre el grupo objetivo seleccionado, cifra la cookie e incluye la cookie en la respuesta al cliente. El cliente debe incluir la cookie que recibe en las solicitudes posteriores al equilibrador de carga. Cuando el equilibrador de carga recibe una solicitud que coincide con una regla con la persistencia del grupo de destino activada y que contiene la cookie, la solicitud se direcciona al grupo de destino especificado en la cookie.

Los equilibradores de carga de aplicaciones no admiten valores de cookies codificados como URL.

Con las solicitudes CORS (intercambio de recursos de varios orígenes), algunos navegadores requieren `SameSite=None; Secure` para habilitar la persistencia. En este caso, Elastic Load Balancing genera una segunda cookie AWSALBTGCORS, que incluye la misma información que la cookie de adherencia original más este `SameSite` atributo. Los clientes reciben ambas cookies.

Example Ejemplo de acción de reenvío con un grupo de destino

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 las solicitudes al grupo de destino especificado.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/my-targets/73e2d6bc24d8a067"
              }
          ]
      }
  }
]
```

Example Ejemplo de acción de reenvío con dos grupos de destino ponderados

La siguiente acción reenvía las solicitudes a los dos grupos de destino especificados, basándose en la ponderación de cada grupo de destino.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/blue-targets/73e2d6bc24d8a067",
                  "Weight": 10
              },
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/green-targets/09966783158cda59",
                  "Weight": 20
              }
          ]
      }
  }
]
```

Example Ejemplo de acción de reenvío con la persistencia activada

Si tiene una acción de reenvío con varios grupos de destino y uno o más de ellos tienen habilitadas las sesiones persistente, debe habilitar la persistencia del grupo de destino.

La siguiente acción reenvía las solicitudes a los dos grupos de destino especificados, con la persistencia del grupo de destino activada. Las solicitudes que no contienen la cookie de permanencia se enrutan en función de la ponderación de cada grupo de destino.

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/blue-targets/73e2d6bc24d8a067",
                  "Weight": 10
```

```
            },
            {
                "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/green-targets/09966783158cda59",
                "Weight": 20
            }
        ],
        "TargetGroupStickinessConfig": {
            "Enabled": true,
            "DurationSeconds": 1000
        }
    }
  }
]
```

## 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).

ruta

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: _-.$/~"'@:+.

consulta

Parámetros de la consulta. La longitud máxima es de 128 caracteres.

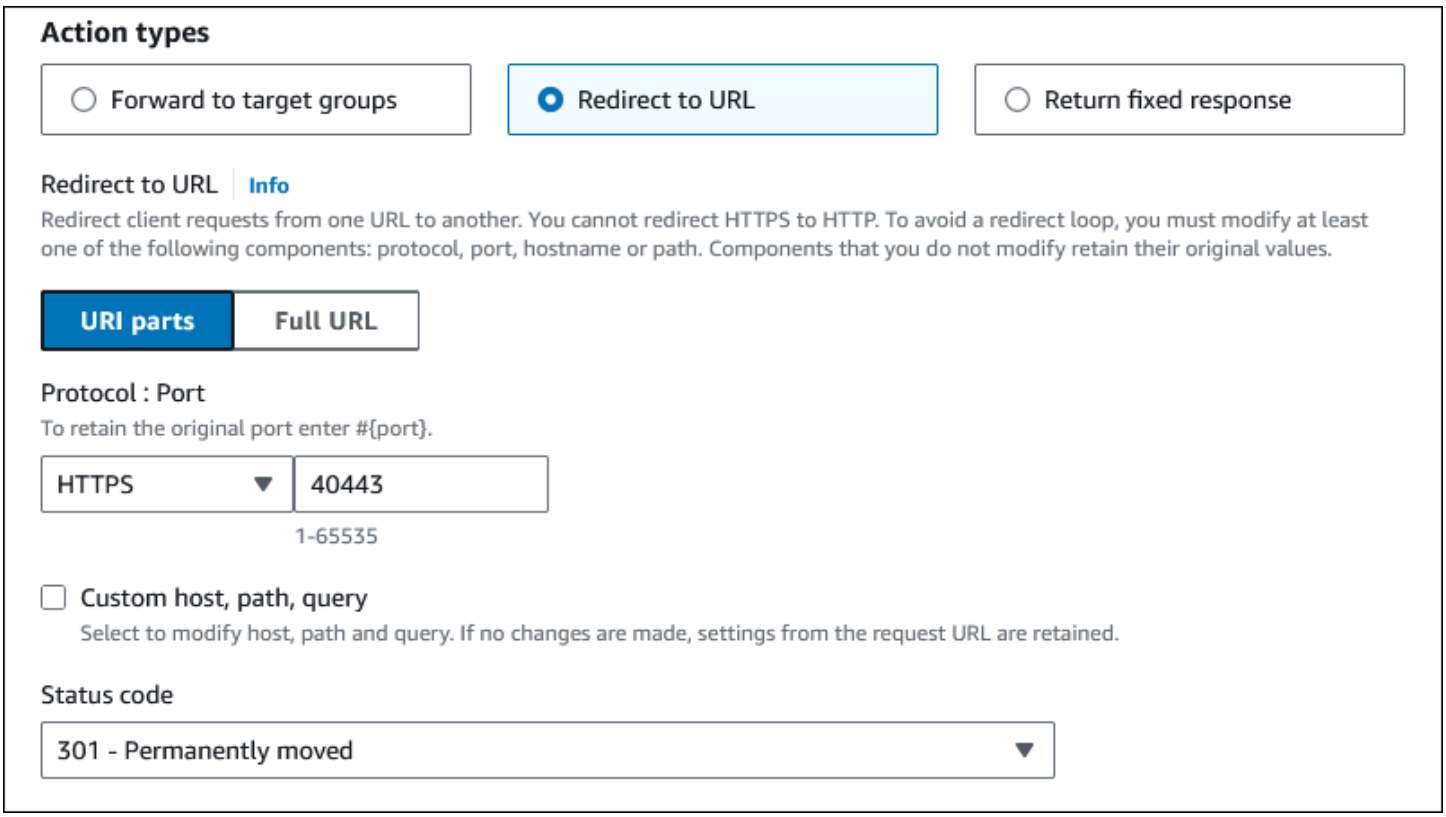
Puede reutilizar los componentes del URI de la URL original en la URL de destino utilizando las siguientes palabras clave reservadas:

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

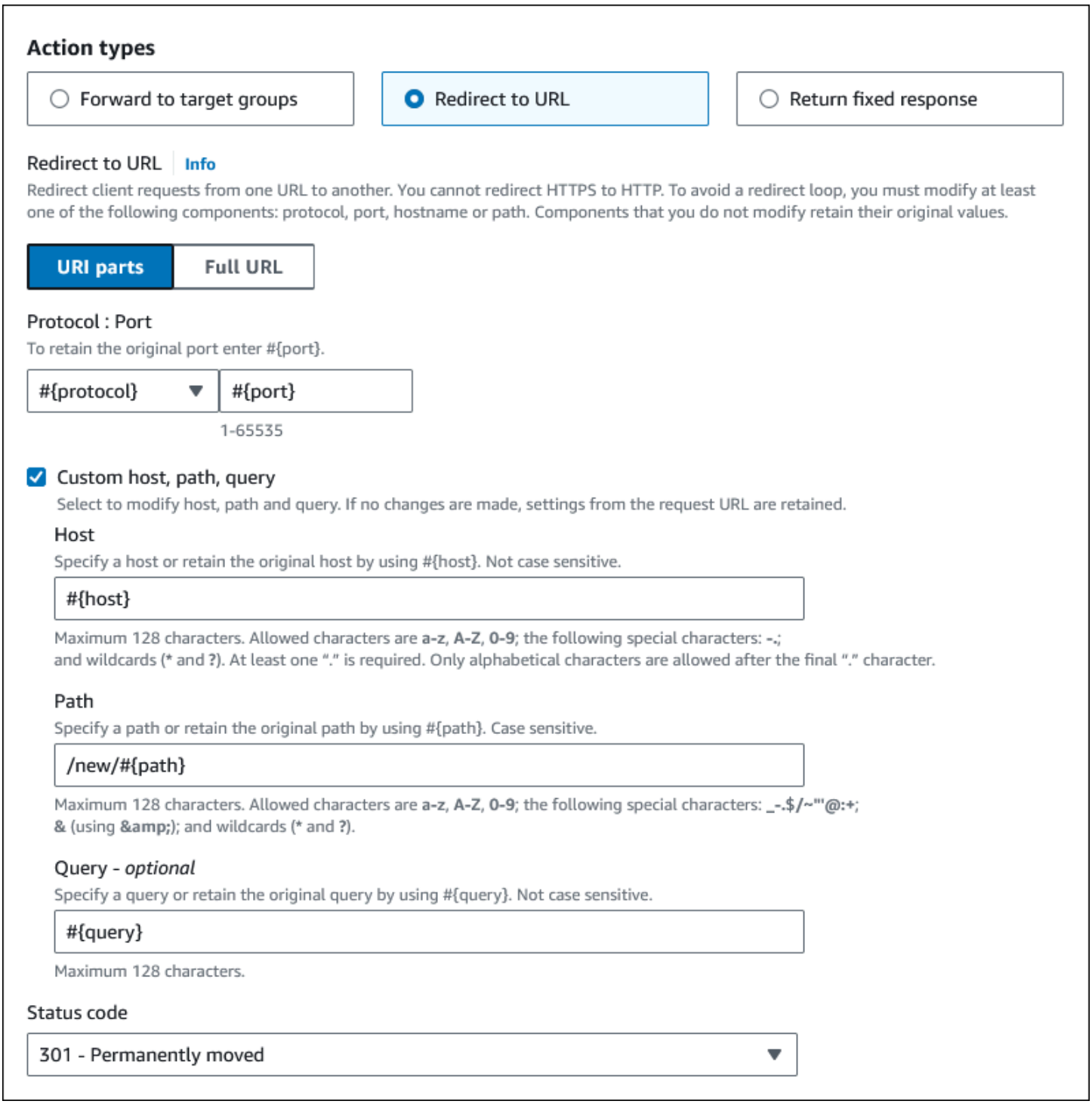
Cuando se ejecuta una acción `redirect`, esta acción se graba en los registros de acceso. Para obtener más información, consulte Entradas de los registros de acceso. El número de acciones `redirect` correctas se registra en la métrica `HTTP_Redirect_Count`. Para obtener más información, consulte Métricas del Equilibrador de carga de aplicación.

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 redireccionamiento para el 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 en función de el nombre de host de cada solicitud. Para obtener más información, consulte Condiciones de host.

`http-header`

Ruta en función de los encabezados HTTP de cada solicitud. Para obtener más información, consulte Condiciones de los encabezados HTTP.

`http-request-method`

Ruta en función de el método de solicitud HTTP de cada solicitud. Para obtener más información, consulte Condiciones de método de solicitud HTTP.

`path-pattern`

Ruta basada en los patrones de ruta de la solicitud URLs. Para obtener más información, consulte Condiciones de ruta.

`query-string`

Ruta basada en key/value pares o valores de las cadenas de consulta. Para obtener más información, consulte Condiciones de cadena de consulta.

`source-ip`

Ruta en función de la dirección IP de origen de cada solicitud. Para obtener más información, consulte Condiciones de dirección IP de origen.

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

Las reglas se aplican solo a los caracteres ASCII visibles; se excluyen los caracteres de control (0x00 a 0x1f y 0x7f).

Para ver demostraciones, consulte Direccionamiento de solicitudes avanzado.

## 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.

Cuando el atributo Application Load Balancer `routing.http.drop_invalid_header_fields` esté habilitado, eliminará los nombres de encabezado que no se ajusten a las expresiones regulares ()`A-Z,a-z,0-9`. También se pueden agregar nombres de encabezado que no se ajusten a las expresiones regulares.

Example Ejemplo de condición de encabezado HTTP para 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 el 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 subdominios y diferentes dominios de nivel superior a través de un único equilibrador de carga.

Los nombre de host no 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 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. Se aplica solo a los caracteres ASCII visibles; se excluyen los caracteres de control (0x00 a 0x1f y 0x7f).

La evaluación de la regla se realiza solo después de que se produzca la normalización del URI.

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)

Si la versión del protocolo es gRPC, las condiciones pueden ser específicas de un paquete, un servicio o un método.

Ejemplos de patrones de ruta HTTP

- `/img/*`
- `/img/*/pics`

Ejemplos de patrones de ruta gRPC

- /package

- /package.service
- /package.service/method

El patrón de ruta se utiliza para direccionar solicitudes, no para modificarlas. Por ejemplo, si una ruta tiene el patrón de `/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 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 usar las condiciones de la cadena de consulta para configurar reglas que enruten las solicitudes en función de los key/value pares o valores de 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 AWS CLI

Puede especificar condiciones al crear o modificar una regla. Para obtener más información, consulte los comandos create-rule y modify-rule. Las solicitudes con una cadena de consulta que incluya un key/value par de «version=v1" o cualquier clave configurada como «ejemplo» cumplen la siguiente condición.

```
[
  {
      "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 ambas IPv4 direcciones y. IPv6 No se admiten caracteres comodín. No puede especificar el CIDR `255.255.255.255/32` para la condición de la regla IP de origen.

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

Las direcciones del X-Forwarded-For encabezado no cumplen esta condición. Para buscar direcciones en el X-Forwarded-For encabezado, utilice una `http-header` condición.

Example Ejemplo de condición de IP de origen para 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"]
      }
  }
]
```

# Encabezados HTTP y balanceadores de tipo equilibrador de carga de aplicaciones

Las solicitudes y respuestas HTTP utilizan campos de encabezado para enviar información sobre los mensajes HTTP. Los encabezados HTTP se añaden automáticamente. Los campos de encabezado son pares nombre-valor separados por signos de dos puntos, separados a su vez por un retorno de carro (CR) y un salto de línea (LF). Un conjunto estándar de campos de encabezado HTTP se define en RFC 2616, Encabezados de mensaje. También hay encabezados HTTP no estándar disponibles que se agregan automáticamente y que se suelen utilizar ampliamente en las aplicaciones. Algunos de los encabezados HTTP no estándar tienen un prefijo `X-Forwarded`. Los Equilibradores de carga de aplicación admiten los siguientes encabezados `X-Forwarded`.

Para obtener más información acerca de las conexiones HTTP, consulte Enrutamiento de solicitudes en la Guía del usuario de Elastic Load Balancing.

Encabezados X-Forwarded

- X-Forwarded-For
- X-Forwarded-Proto
- X-Forwarded-Port

## X-Forwarded-For

El encabezado de solicitud `X-Forwarded-For` ayuda a identificar la dirección IP de un cliente cuando se utiliza un equilibrador de carga HTTP o HTTPS. Dado que los equilibradores de carga interceptan el tráfico entre los clientes y los servidores, los registros de acceso al servidor contienen únicamente la dirección IP del equilibrador de carga. Para ver la dirección IP del cliente, utilice el atributo `routing.http.xff_header_processing.mode`. Este atributo permite modificar, conservar o eliminar el encabezado `X-Forwarded-For` en la solicitud HTTP antes de que el Equilibrador de carga de aplicación envíe la solicitud al destino. Los valores posibles para este atributo son `append`, `preserve` y `remove`. El valor predeterminado de este atributo es `append`.

> **Important**
>
> El encabezado `X-Forwarded-For` debe usarse con precaución debido a los posibles riesgos de seguridad. Las entradas solo pueden considerarse fiables si las agregan sistemas que estén debidamente protegidos dentro de la red.

## Anexar

De manera predeterminada, el Equilibrador de carga de aplicación almacena la dirección IP del cliente en el encabezado de solicitud `X-Forwarded-For` y se lo pasa al encabezado de su servidor. Si el encabezado de solicitud `X-Forwarded-For` no se incluye en la solicitud original, el equilibrador de carga crea uno con la dirección IP del cliente como el valor de la solicitud. De lo contrario, el equilibrador de carga agrega la dirección IP del cliente al encabezado existente y se lo pasa al servidor. El encabezado de solicitud `X-Forwarded-For` puede contener varias direcciones IP separadas por comas.

El encabezado de solicitud `X-Forwarded-For` tiene el siguiente formato:

```
X-Forwarded-For: client-ip-address
```

A continuación se muestra un ejemplo de un encabezado de solicitud `X-Forwarded-For` cuya dirección IP de cliente es `203.0.113.7`.

```
X-Forwarded-For: 203.0.113.7
```

A continuación se muestra un ejemplo de encabezado de `X-Forwarded-For` solicitud para un cliente con una IPv6 dirección de`2001:DB8::21f:5bff:febf:ce22:8a2e`.

```
X-Forwarded-For: 2001:DB8::21f:5bff:febf:ce22:8a2e
```

Cuando el atributo de conservación del puerto del cliente (`routing.http.xff_client_port.enabled`) está habilitado en el equilibrador de carga, el encabezado de la solicitud `X-Forwarded-For` incluye el atributo `client-port-number` adjunto al atributo `client-ip-address`, separado por dos puntos. El encabezado luego tiene el siguiente formato:

```
IPv4 -- X-Forwarded-For: client-ip-address:client-port-number
```

```
IPv6 -- X-Forwarded-For: [client-ip-address]:client-port-number
```

Por IPv6 ejemplo, ten en cuenta que cuando el balanceador de cargas añade la dirección `client-ip-address` al encabezado existente, incluye la dirección entre corchetes.

A continuación se muestra un ejemplo de encabezado de `X-Forwarded-For` solicitud para un cliente con una IPv4 dirección `12.34.56.78` y un número de puerto de. `8080`

```
X-Forwarded-For: 12.34.56.78:8080
```

A continuación se muestra un ejemplo de encabezado de `X-Forwarded-For` solicitud para un cliente con una IPv6 dirección `2001:db8:85a3:8d3:1319:8a2e:370:7348` y un número de puerto de`8080`.

```
X-Forwarded-For: [2001:db8:85a3:8d3:1319:8a2e:370:7348]:8080
```

### Conservar

El modo `preserve` del atributo garantiza que el encabezado `X-Forwarded-For` de la solicitud HTTP no se modifique de ninguna manera antes de enviarse a los destinos.

### Quitar

El modo `remove` del atributo elimina el encabezado `X-Forwarded-For` de la solicitud HTTP antes de enviarla a los destinos.

> **Note**
>
> Si habilita el atributo de conservación del puerto del cliente (`routing.http.xff_client_port.enabled`) y también selecciona `preserve` o `remove` para el atributo `routing.http.xff_header_processing.mode`, el Equilibrador de carga de aplicación anula el atributo de conservación del puerto del cliente. Mantiene el encabezado `X-Forwarded-For` sin cambios o lo elimina según el modo que seleccione antes de enviarlo a los destinos.

En la siguiente tabla se muestran ejemplos del encabezado `X-Forwarded-For` que recibe el destino al seleccionar el modo `append`, `preserve` o el modo `remove`. En este ejemplo, la dirección IP de la última transferencia es `127.0.0.1`.

| Descripción de la solicitud | Ejemplo de solicitud | XFF en modo **append** | XFF en modo **preserve** | XFF en modo **remove** |
|---|---|---|---|---|
| La solicitud se envía sin encabezado XFF | `GET / index.html HTTP/1.1 Host: example.com` | `X-Forwarded-For: 127.0.0.1` | No presente | No presente |
| La solicitud se envía con un encabezado XFF y una dirección IP de cliente. | `GET / index.html HTTP/1.1 Host: example.com X-Forwarded-For: 127.0.0.4` | `X-Forwarded-For: 127.0.0.4, 127.0.0.1` | `X-Forwarded-For: 127.0.0.4` | No presente |
| La solicitud se envía con un encabezado XFF con varias direcciones IP de cliente. | `GET / index.html HTTP/1.1 Host: example.com X-Forwarded-For: 127.0.0.4, 127.0.0.8` | `X-Forwarded-For: 127.0.0.4, 127.0.0.8, 127.0.0.1` | `X-Forwarded-For: 127.0.0.4, 127.0.0.8` | No presente |

Para modificar, conservar o eliminar el encabezado X-Forwarded-For mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.

5. En la sección de configuración del tráfico, en Gestión de paquetes, en el X-Forwarded-For encabezado, selecciona Añadir (predeterminado), Conservar o Eliminar.
6. Seleccione Save changes (Guardar cambios).

Para modificar, conservar o eliminar el X-Forwarded-For encabezado mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes con el atributo `routing.http.xff_header_processing.mode`.

## X-Forwarded-Proto

El encabezado de solicitud `X-Forwarded-Proto` ayuda a identificar el protocolo (HTTP o HTTPS) que un cliente utiliza para conectarse al equilibrador de carga. Los registros de acceso al servidor contienen únicamente el protocolo que se utiliza entre el servidor y el equilibrador de carga; sin embargo, no contienen información sobre el protocolo utilizado entre el cliente y el equilibrador de carga. Para determinar el protocolo utilizado entre el cliente y el equilibrador de carga, utilice el encabezado de solicitud `X-Forwarded-Proto`. Elastic Load Balancing almacena el protocolo utilizado entre el cliente y el equilibrador de carga en el encabezado de solicitud `X-Forwarded-Proto` y se lo pasa al servidor.

La aplicación o el sitio web pueden utilizar el protocolo almacenado en el encabezado de solicitud `X-Forwarded-Proto` para generar una respuesta que redirija a la URL correspondiente.

El encabezado de solicitud `X-Forwarded-Proto` tiene el siguiente formato:

```
X-Forwarded-Proto: originatingProtocol
```

El siguiente ejemplo contiene un encabezado de solicitud `X-Forwarded-Proto` correspondiente a una solicitud originada en el cliente como solicitud HTTPS:

```
X-Forwarded-Proto: https
```

## X-Forwarded-Port

El encabezado de solicitud `X-Forwarded-Port` ayuda a identificar el puerto de destino que el cliente utiliza para conectarse al equilibrador de carga.

# Crear un oyente HTTP para su equilibrador de carga de aplicaciones

Un oyente verifica solicitudes de conexión. Los oyentes se definen cuando se crea el equilibrador de carga, pero se pueden agregar otros oyentes en cualquier momento.

La información de esta página le ayuda a crear un oyente HTTP para su equilibrador de carga. Para agregar un oyente HTTPS a su equilibrador de carga, consulte Crear un oyente HTTPS para el equilibrador de carga de aplicaciones

## Requisitos previos

- Para añadir una acción de reenvío a la regla predeterminada del oyente, debe especificar un grupo de destino disponible. Para obtener más información, consulte Creación de un grupo de destino para el Equilibrador de carga de aplicación.
- Puede especificar el mismo grupo de destino en varios oyentes, pero estos deben pertenecer al mismo equilibrador de carga. Para usar un grupo de destino con un equilibrador de carga, debe comprobar que un oyente no lo use para ningún otro equilibrador de carga.

## Agregar un oyente HTTP

Los oyentes se configuran con un protocolo y un puerto para las conexiones entre los clientes y el equilibrador de carga, así como un grupo de destino para la regla predeterminada del oyente. Para obtener más información, consulte Configuración del oyente.

Cómo agregar un oyente HTTPS utilizando la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, seleccione Añadir oyente.
5. En Protocolo: puerto, elija HTTP y mantenga el puerto predeterminado o introduzca un puerto distinto.
6. En Acciones predeterminadas, elija una de las siguientes opciones:

- Reenviar a los grupos de destino: seleccione uno o más grupos de destino a los que reenviar el tráfico. Para añadir grupos de destino, seleccione Añadir grupo de destino. Si utiliza más de un grupo de destino, seleccione una ponderación para cada uno y revise el porcentaje asociado. Debe habilitar la persistencia a nivel de grupo en una regla, si se activó la persistencia en uno o más de los grupos de destino.
- Redirigir a la URL: especifique la URL a la que se redirigirán las solicitudes de los clientes. Esto se puede hacer al introducir cada parte por separado en la pestaña partes de la URI o al ingrsear la dirección completa en la pestaña URL completa. Puede configurar las acciones de redirección como temporales (HTTP 302) o permanentes (HTTP 301), en función de sus necesidades para Código de estado.
- Devolver una respuesta fija: especifique el código de respuesta que se devolverá a las solicitudes de los clientes rechazadas. Además, puede especificar el Tipo de contenido y el Cuerpo de la respuesta, pero no son obligatorios.

7. Elija Agregar.

Para añadir un agente de escucha HTTP mediante el AWS CLI

Utilice el comando create-oyente para crear el oyente y la regla predeterminada, y el comando create-rule para definir nuevas reglas del oyente.

# Certificados SSL para el Equilibrador de carga de aplicación

Cuando crea un oyente seguro para el Equilibrador de carga de aplicación, debe implementar al menos un certificado en el equilibrador de carga. El equilibrador 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 equilibrador de carga, debe especificar un nombre de dominio. El nombre de dominio del certificado debe coincidir con el registro del nombre de dominio personalizado para poder verificar la conexión TLS. Si no coinciden, no se cifrará el tráfico.

Debe especificar un nombre de dominio completo (FQDN) para el certificado, por ejemplo, `www.example.com`, o bien un nombre de dominio de ápex, por ejemplo, `example.com`. También puede utilizar un asterisco (*) como comodín para proteger varios nombres de sitios del mismo dominio. Cuando se solicita un certificado comodín, el asterisco (*) debe encontrarse en la posición

situada más a la izquierda del nombre de dominio, y solo puede proteger un nivel de subdominio. Por ejemplo, `*.example.com` protege `corp.example.com` y `images.example.com`, pero no puede proteger `test.login.example.com`. Además, tenga en cuenta que `*.example.com` solo protege los subdominios de `example.com`; no protege el dominio desnudo o ápex (`example.com`). El nombre del caracter comodín aparecerá en el campo Sujeto y en la extensión Nombre alternativo del sujeto del certificado. Para obtener más información sobre los certificados públicos, consulte Solicitar un certificado público en la Guía del AWS Certificate Manager usuario.

Le recomendamos que utilice AWS Certificate Manager (ACM) para crear los certificados del equilibrador de carga. ACM es compatible con los certificados RSA con longitudes de clave de 2048, 3072 y 4096 bits, y con todos los certificados ECDSA. ACM se integra con Elastic Load Balancing, lo que le permite implementar el certificado en el equilibrador de carga. Para obtener más información, consulte la Guía del usuario de AWS Certificate Manager.

Como alternativa, puede utilizar SSL/TLS las herramientas para crear una solicitud de firma de certificados (CSR) y, a continuación, conseguir que una CA firme la CSR para generar un certificado y, a continuación, importar el certificado a 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 oyente HTTPS, debe especificar exactamente un certificado. Este certificado se conoce como certificado predeterminado. Puede sustituir el certificado predeterminado después de crear el oyente HTTPS. Para obtener más información, consulte Reemplazar el certificado predeterminado.

Si especifica certificados adicionales en una lista de certificados, 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 equilibrador de carga, puede utilizar un certificado comodín o añadir un nombre alternativo de asunto (SAN) para cada dominio adicional al certificado.

## Lista de certificados

Tras crear un agente de escucha HTTPS, puede añadir certificados a la lista de certificados. Si creó el agente de escucha con el AWS Management Console, agregamos el certificado predeterminado

a la lista de certificados por usted. De lo contrario, la lista de certificados está vacía. El uso de una lista de certificados permite al equilibrador de carga admitir varios dominios en el mismo puerto y proporcionar un certificado diferente para cada dominio. Para obtener más información, consulte Añadir certificados a la lista de certificados.

El equilibrador 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 equilibrador de carga selecciona este certificado. Si un nombre de host proporcionado por un cliente coincide con varios certificados de la lista de certificados, el equilibrador 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)
- Vencimiento (se prefiere que no esté vencido)
- Algoritmo de hash (prefiera el SHA antes que el SHA MD5). Si hay varios certificados SHA, prefiera el número SHA más alto.
- Longitud de clave (prefieren la mayor)
- Periodo de validez

Las entradas del registro de acceso del equilibrador 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 registros de acceso.

## Renovación de certificados

Cada certificado viene con un periodo de validez. Debe asegurarse de renovar o reemplazar cada certificado para su equilibrador 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 equilibrador 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 AWS Certificate Manager e implementados en el balanceador de cargas se pueden renovar automáticamente. ACM intenta renovar los certificados antes de que

venzan. Para obtener más información, consulte Renovación administrada en la Guía del usuario de AWS Certificate Manager .

- Si el certificado se importó en ACM, deberá monitorear la fecha de vencimiento del certificado y renovarlo antes de que venza. Para obtener más información, consulte Importación de 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 equilibrador de carga y eliminar el certificado caducado del equilibrador de carga.

# Políticas de seguridad para el Equilibrador de carga de aplicación

Elastic Load Balancing utiliza una configuración de negociación de capa de conexión segura (SSL), conocida como política de seguridad, para negociar las conexiones SSL entre un cliente y el equilibrador 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 equilibrador 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 equilibrador 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.

Consideraciones

- Los Equilibradores de carga de aplicación solo admiten la renegociación de SSL para las conexiones de destino.
- Al crear un oyente HTTPS, debe seleccionar una política de seguridad.
- La política `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` es la política de seguridad predeterminada para los oyentes de HTTPS creada con la AWS Management Console. Esta política es compatible con TLS 1.3 y es compatible con versiones anteriores de TLS 1.2.
- La política `ELBSecurityPolicy-2016-08` es la política de seguridad predeterminada para los oyentes de HTTPS creada con la AWS CLI.
- Los equilibradores de carga de aplicaciones no admiten políticas de seguridad personalizadas.

- Puede seleccionar la política de seguridad que se utiliza para las conexiones frontend, pero no para las conexiones backend.
  - En el caso de las conexiones de backend, si alguno de sus oyentes de HTTPS utiliza una política de seguridad de TLS 1.3, se utilizará la política de seguridad `ELBSecurityPolicy-TLS13-1-0-2021-06`. De lo contrario, la política de seguridad `ELBSecurityPolicy-2016-08` se utiliza con las conexiones de backend.
  - Nota: Si utilizas una política TLS de FIPS en tu agente de escucha HTTPS, `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` se utiliza para las conexiones de back-end.
- A fin de 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, puede usar una de las políticas de seguridad `ELBSecurityPolicy-TLS-`. Para ver la versión del protocolo TLS para las solicitudes dirigidas al Equilibrador de carga de aplicación, habilite el registro de acceso del equilibrador de carga y examine las entradas de los registros de acceso correspondientes. Para obtener más información, consulte Registros de acceso del Equilibrador de carga de aplicación.
- Puede restringir las políticas de seguridad que están disponibles para los usuarios en sus políticas de IAM Cuentas de AWS y control de servicios () y AWS Organizations mediante ellas mediante las claves de condición de Elastic Load Balancing en sus políticas de IAM y de control de servicios (SCPs), respectivamente. Para obtener más información, consulte las políticas de control de servicios (SCPs) en la Guía del AWS Organizations usuario
- Las políticas que solo admiten TLS 1.3 admiten el secreto directo (FS). Las políticas compatibles con TLS 1.3 y TLS 1.2 que solo tienen cifrados del formato TLS_* y ECDHE_* también proporcionan FS.
- Los balanceadores de carga de aplicaciones admiten la reanudación de TLS mediante PSK (TLS 1.3) y tickets de sesión (TLS 1.2 y versiones anteriores). IDs/session Las reanudaciones solo se admiten en conexiones a la misma dirección IP del Equilibrador de carga de aplicación. La característica 0-RTT Data y la extensión early_data no están implementadas.
- Los balanceadores de carga de aplicaciones admiten la extensión Extended Master Secret (EMS) para TLS 1.2.

Puede describir los protocolos y los cifrados mediante el describe-ssl-policies AWS CLI comando o consultar las tablas siguientes.

Políticas de seguridad

# Políticas de seguridad de TLS

Puede utilizar las políticas de seguridad de TLS para ajustarse a los estándares de seguridad y conformidad que requieren que se deshabiliten ciertas versiones del protocolo TLS, o bien para admitir clientes heredados que requieren cifrados obsoletos.

Las políticas que solo admiten TLS 1.3 admiten el secreto directo (FS). Las políticas compatibles con TLS 1.3 y TLS 1.2 que solo tienen cifrados del formato TLS_* y ECDHE_* también proporcionan FS.

Contenido



## Protocolos por política

En la siguiente tabla se detallan los protocolos que admite cada política de seguridad TLS.

| Políticas de seguridad | TLS 1.3 | TLS 1.2 | TLS 1.1 | TLS 1.0 |
|---|---|---|---|---|
| ELBSecurityPolítica- -1-3-2021-06 TLS13 | Sí | No | No | No |
| ELBSecurityPolítica- TLS13 -1-2-2021-06 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-2-Res-2021-06 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-2-Ext2-2021-06 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-2-Ext1-2021-06 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-1-2021-06 | Sí | Sí | Sí | No |
| ELBSecurityPolítica- TLS13 -1-0-2021-06 | Sí | Sí | Sí | Sí |
| ELBSecurityPolítica-TLS-1-2-EXT-2018-06 | No | Sí | No | No |
| ELBSecurityPolítica-TLS-1-2-2017-01 | No | Sí | No | No |
| ELBSecurityPolítica-TLS-1-1-2017-01 | No | Sí | Sí | No |
| ELBSecurityPolítica-2016-08 | No | Sí | Sí | Sí |
| ELBSecurityPolítica-2015-05 | No | Sí | Sí | Sí |

## Cifrados por política

En la siguiente tabla se detallan los cifrados que admite cada política de seguridad TLS.

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-3-2021-06 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 |
| ELBSecurityPolítica- TLS13 -1-2-2021-06 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• TLS_ 0_ 05_ CHACHA2 POLY13 SHA256<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- -GCM AES256 - SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384 |
| ELBSecurityPolítica- -1-2-Res-2021-06 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• TLS_ 0_ 05_ CHACHA2 POLY13 SHA256<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384 |
| ELBSecurityPolítica- TLS13 -1-2-Ext2-2021-06 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• TLS_ 0_ 05_ CHACHA2 POLY13 SHA256<br>• ECDHE-ECDSA- -GCM- AES128 SHA256 |

| Política de seguridad | Cifrados |
| --- | --- |
| | • ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-ECDSA- AES256 -SHA<br>• ECDHE-RSA- -SHA AES256<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-2-Ext1-2021-06 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• TLS_ 0_ 05_ CHACHA2 POLY13 SHA256<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- -GCM AES256 - SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES256-GCM- SHA384<br>• AES256-SHA256 |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-1-2021-06 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• TLS_ 0_ 05_ CHACHA2 POLY13 SHA256<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-ECDSA- AES256 -SHA<br>• ECDHE-RSA- -SHA AES256<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-0-2021-06 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• TLS_ 0_ 05_ CHACHA2 POLY13 SHA256<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-ECDSA- AES256 -SHA<br>• ECDHE-RSA- -SHA AES256<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica-TLS-1-2-EXT-2018-06 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-ECDSA- AES256 -SHA<br>• ECDHE-RSA- -SHA AES256<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica-TLS-1-2-2017-01 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- -GCM AES256 - SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES256-GCM- SHA384<br>• AES256-SHA256 |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica-TLS-1-1-2017-01 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-ECDSA- AES256 -SHA<br>• ECDHE-RSA- -SHA AES256<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica-2016-08 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-ECDSA- AES256 -SHA<br>• ECDHE-RSA- -SHA AES256<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica-2015-05 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-ECDSA- AES256 -SHA<br>• ECDHE-RSA- -SHA AES256<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

## Políticas por cifrado

En la siguiente tabla se detallan las políticas de seguridad TLS que admiten cada cifrado.

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL: TLS_AES_128_GCM_ SHA256<br><br>IANA — TLS_AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-3-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-2021 -06 | 1301 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
|---|---|---|
| | • ELBSecurityPolítica- TLS13 -1-2-Res-2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06 | |
| OpenSSL: TLS_AES_256_GCM_ SHA384<br><br>IANA — TLS_AES_256_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-3-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Res-2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06 | 1302 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — TLS_ 0_ 05_ CHACHA2 POLY13 SHA256<br><br>IANA — TLS_ CHACHA2 0_ POLY13 05_ SHA256 | • ELBSecurityPolítica- TLS13 -1-3-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Res- 2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06 | 1303 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 128-GCM - ECDHE-ECDSA-AES SHA256<br><br>IANA — TLS_ECDHE_ECDSA_CON_AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Res-2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2-2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1-2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021-06<br>• ELBSecurityPolítica- TLS13 -1-0-2021-06<br>• ELBSecurityPolítica-TLS-1-2-EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c02b |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 128-GCM - ECDHE-RSA-AES SHA256<br><br>IANA — TLS_ECDHE_RSA_CON_ AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Res-2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2-EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c02f |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 128- ECDHE-ECDSA-AES SHA256<br><br>IANA — TLS_ECDHE_ECDSA_CO N_AES_128_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c023 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 128- ECDHE-RSA-AES SHA256<br><br>IANA — TLS_ECDHE_RSA_CON_ AES_128_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c027 |
| ECDHE-ECDSA-AESOpenSSL: 128- SHA<br><br>IANA: TLS_ECDHE_ECDSA_WI TH_AES_128_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c009 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| ECDHE-RSA-AESOpenSSL: 128-SHA<br><br>IANA: TLS_ECDHE_RSA_WITH _AES_128_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c013 |
| OpenSSL — 256-GCM - ECDHE-ECD SA-AES SHA384<br><br>IANA — TLS_ECDHE_ECDSA_CO N_AES_256_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Res- 2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c02c |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 256-GCM - ECDHE-RSA-AES SHA384<br><br>IANA — TLS_ECDHE_RSA_CON_ AES_256_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Res-2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2-EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c030 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 256- ECDHE-ECDSA-AES SHA384<br><br>IANA — TLS_ECDHE_ECDSA_CO N_AES_256_CBC_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c024 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 256- ECDHE-RSA-AES SHA384<br><br>IANA — TLS_ECDHE_RSA_CON_ AES_256_CBC_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c028 |
| ECDHE-ECDSA-AESOpenSSL: 256- SHA<br><br>IANA: TLS_ECDHE_ECDSA_WI TH_AES_256_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c00a |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| ECDHE-RSA-AESOpenSSL: 256-SHA<br><br>IANA: TLS_ECDHE_RSA_WITH _AES_256_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | c014 |
| OpenSSL — -GCM- AES128 SHA256<br><br>IANA — TLS_RSA_CON_AES_12 8_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | 9c |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — - AES128 SHA256<br><br>IANA — TLS_RSA_CON_AES_12 8_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | 3c |
| OpenSSL — SHA AES128<br><br>IANA: TLS_RSA_WITH_AES_1 28_CBC_SHA | • ELBSecurityPolítica- -1-2-Ext2 -2021-06 TLS13<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | 2f |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — -GCM- AES256 SHA384<br><br>IANA — TLS_RSA_CON_AES_25 6_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | 9d |
| OpenSSL — - AES256 SHA256<br><br>IANA — TLS_RSA_CON_AES_25 6_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-Ext2 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-2-Ext1 -2021-06<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2- EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-2-2017-01<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | 3d |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — SHA AES256<br><br>IANA: TLS_RSA_WITH_AES_256_CBC_SHA | • ELBSecurityPolítica- -1-2-Ext2 -2021-06 TLS13<br>• ELBSecurityPolítica- TLS13 -1-1-2021 -06<br>• ELBSecurityPolítica- TLS13 -1-0-2021 -06<br>• ELBSecurityPolítica-TLS-1-2-EXT-2018-06<br>• ELBSecurityPolítica-TLS-1-1-2017-01<br>• ELBSecurityPolítica-2016-08 | 35 |

## Políticas de seguridad FIPS

> **Important**
>
> Todos los oyentes seguros conectados a un Equilibrador de carga de aplicación deben usar políticas de seguridad FIPS o políticas de seguridad que no sean FIPS; recuerde que no se pueden mezclar. Si un Equilibrador de carga de aplicación existente tiene dos o más oyentes que utilizan políticas que no son FIPS y desea que los oyentes usen políticas de seguridad FIPS en su lugar, elimine todos los oyentes hasta que solo quede uno. Cambie la política de seguridad del oyente a FIPS y, a continuación, cree más oyentes mediante las políticas de seguridad de FIPS. Como alternativa, puede crear un nuevo Equilibrador de carga de aplicación con nuevos oyentes utilizando únicamente las políticas de seguridad FIPS.

El Estándar de procesamiento de la información federal (FIPS) es un estándar de seguridad de los gobiernos de EE. UU. y Canadá que especifica los requisitos de seguridad de los módulos criptográficos que protegen información confidencial. Para obtener más información, consulte Estándar de procesamiento de la información federal (FIPS) 140-3 en la página Conformidad de Seguridad en la nube de AWS .

Todas las políticas FIPS utilizan el módulo criptográfico AWS-LC validado para FIPS. Para obtener más información, consulte la página del módulo criptográfico AWS-LC en el sitio NIST Cryptographic Module Validation Program.

> **Important**
>
> Las políticas `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` y `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` se proporcionan únicamente para ofrecer compatibilidad con versiones heredadas. Si bien utilizan la criptografía FIPS mediante el módulo FIPS14 0, es posible que no se ajusten a las directrices más recientes del NIST para la configuración de TLS.

Contenido



## Protocolos por política

En la siguiente tabla se detallan los protocolos que admite cada política de seguridad FIPS.

| Políticas de seguridad | TLS 1.3 | TLS 1.2 | TLS 1.1 | TLS 1.0 |
|---|---|---|---|---|
| ELBSecurityTLS13Política- -1-3-FIPS-2023-04 | Sí | No | No | No |
| ELBSecurityPolítica- TLS13 -1-2-FIPS-2023-04 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-2-RES-FIPS-2023-04 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04 | Sí | Sí | No | No |

| Políticas de seguridad | TLS 1.3 | TLS 1.2 | TLS 1.1 | TLS 1.0 |
|---|---|---|---|---|
| ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04 | Sí | Sí | No | No |
| ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04 | Sí | Sí | Sí | No |
| ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | Sí | Sí | Sí | Sí |

## Cifrados por política

En la siguiente tabla se detallan los cifrados que admite cada política de seguridad FIPS.

| Política de seguridad | Cifrados |
|---|---|
| ELBSecurityPolítica- TLS13 -1-3-FIPS-2023-04 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384 |
| ELBSecurityPolítica- -1-2-FIPS-2023-04 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- -GCM AES256 - SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384 |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-2-RES-FIPS-2023-04 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384 |
| ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-RSA- AES256 -SHA<br>• ECDHE-ECDSA- AES256 -SHA<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-2-EXT1-FIPS-2023-04 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- -GCM AES256 - SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES256-GCM- SHA384<br>• AES256-SHA256 |
| ELBSecurityPolítica- -1-2-EXT0-FIPS-2023-04 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-RSA- AES256 -SHA<br>• ECDHE-ECDSA- AES256 -SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-1-FIPS-2023-04 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-RSA- AES256 -SHA<br>• ECDHE-ECDSA- AES256 -SHA<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica- -1-0-FIPS-2023-04 TLS13 | • TLS_AES_128_GCM_ SHA256<br>• TLS_AES_256_GCM_ SHA384<br>• ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-RSA- AES256 -SHA<br>• ECDHE-ECDSA- AES256 -SHA<br>• AES128-GCM- SHA256<br>• AES128-SHA256<br>• AES128-SHA<br>• AES256-GCM- SHA384<br>• AES256-SHA256<br>• AES256-SHA |

## Políticas por cifrado

En la siguiente tabla se detallan las políticas de seguridad FIPS que admiten cada cifrado.

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL: TLS_AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-3-FIPS -2023-04 | 1301 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| IANA — TLS_AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-RES-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | |
| OpenSSL: TLS_AES_256_GCM_ SHA384<br><br>IANA — TLS_AES_256_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-3-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-RES-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | 1302 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 128-GCM - ECDHE-ECDSA-AES SHA256<br><br>IANA — TLS_ECDHE_ECDSA_CON_AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-RES-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c02b |
| OpenSSL — 128-GCM - ECDHE-RSA-AES SHA256<br><br>IANA — TLS_ECDHE_RSA_CON_AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-RES-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c02f |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 128- ECDHE-ECDSA-AES SHA256<br><br>IANA — TLS_ECDHE_ECDSA_CO N_AES_128_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | c023 |
| OpenSSL — 128- ECDHE-RSA-AES SHA256<br><br>IANA — TLS_ECDHE_RSA_CON_ AES_128_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | c027 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| ECDHE-ECDSA-AESOpenSSL: 128-SHA<br><br>IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-ext2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c009 |
| ECDHE-RSA-AESOpenSSL: 128-SHA<br><br>IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-ext2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c013 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 256-GCM - ECDHE-ECDSA-AES SHA384<br><br>IANA — TLS_ECDHE_ECDSA_CON_AES_256_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-RES-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c02c |
| OpenSSL — 256-GCM - ECDHE-RSA-AES SHA384<br><br>IANA — TLS_ECDHE_RSA_CON_AES_256_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-RES-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c030 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 256- ECDHE-ECDSA-AES SHA384<br><br>IANA — TLS_ECDHE_ECDSA_CO N_AES_256_CBC_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | c024 |
| OpenSSL — 256- ECDHE-RSA-AES SHA384<br><br>IANA — TLS_ECDHE_RSA_CON_ AES_256_CBC_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | c028 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
|---|---|---|
| ECDHE-ECDSA-AESOpenSSL: 256-SHA<br><br>IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-ext2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c00a |
| ECDHE-RSA-AESOpenSSL: 256-SHA<br><br>IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | • ELBSecurityPolítica- TLS13 -1-2-ext2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT0-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | c014 |
| OpenSSL — -GCM- AES128 SHA256<br><br>IANA — TLS_RSA_CON_AES_128_GCM_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS-2023-04 | 9c |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — - AES128 SHA256<br><br>IANA — TLS_RSA_CON_AES_12 8_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2- EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | 3c |
| OpenSSL — SHA AES128<br><br>IANA: TLS_RSA_WITH_AES_1 28_CBC_SHA | • ELBSecurityPolítica- -1-2-ext2- FIPS-2023-04 TLS13<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | 2f |
| OpenSSL — -GCM- AES256 SHA384<br><br>IANA — TLS_RSA_CON_AES_25 6_GCM_ SHA384 | • ELBSecurityPolítica- TLS13 -1-2- EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2- EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | 9d |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
|---|---|---|
| OpenSSL — - AES256 SHA256<br><br>IANA — TLS_RSA_CON_AES_25 6_CBC_ SHA256 | • ELBSecurityPolítica- TLS13 -1-2-EXT2-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-2-EXT1-FIPS-2023-04<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | 3d |
| OpenSSL — SHA AES256<br><br>IANA: TLS_RSA_WITH_AES_2 56_CBC_SHA | • ELBSecurityPolítica- -1-2-ext2-FIPS-2023-04 TLS13<br>• ELBSecurityPolítica- TLS13 -1-1-FIPS -2023-04<br>• ELBSecurityPolítica- TLS13 -1-0-FIPS -2023-04 | 35 |

## Para las políticas admitidas

Las políticas de seguridad compatibles con FS (secreto hacia adelante) proporcionan protecciones adicionales contra el espionaje de datos cifrados mediante el uso de una clave de sesión aleatoria única. Esto impide la decodificación de los datos capturados, incluso si la clave secreta a largo plazo se ve comprometida.

Las políticas de esta sección son compatibles con FS y sus nombres incluyen «FS». Sin embargo, estas no son las únicas políticas que admiten FS. Las políticas que solo admiten TLS 1.3 admiten FS. Las políticas que admiten TLS 1.3 y TLS 1.2 que solo tienen cifrados del formato TLS_* y ECDHE_* también proporcionan FS.

Contenido

## Protocolos por política

En la siguiente tabla se detallan los protocolos que admite cada política de seguridad FS admitida.

| Políticas de seguridad | TLS 1.3 | TLS 1.2 | TLS 1.1 | TLS 1.0 |
|---|---|---|---|---|
| ELBSecurityPolítica-FS-1-2-RES-2020-10 | No | Sí | No | No |
| ELBSecurityPolítica-FS-1-2-RES-2019-08 | No | Sí | No | No |
| ELBSecurityPolítica-FS-1-2-2019-08 | No | Sí | No | No |
| ELBSecurityPolítica-FS-1-1-2019-08 | No | Sí | Sí | No |
| ELBSecurityPolítica-FS-2018-06 | No | Sí | Sí | Sí |

## Cifrados por política

En la siguiente tabla se detallan los cifrados que admite cada política de seguridad FS admitida.

| Política de seguridad | Cifrados |
|---|---|
| ELBSecurityPolítica-FS-1-2-RES-2020-10 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384 |
| ELBSecurityPolítica-FS-1-2-RES-2019-08 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256 |

| Política de seguridad | Cifrados |
| --- | --- |
| | • ECDHE-ECDSA- -GCM AES256 - SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384 |
| ELBSecurityPolítica-FS-1-2-2019-08 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-RSA- AES256 -SHA<br>• ECDHE-ECDSA- AES256 -SHA |
| ELBSecurityPolítica-FS-1-1-2019-08 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-RSA- AES256 -SHA<br>• ECDHE-ECDSA- AES256 -SHA |

| Política de seguridad | Cifrados |
| --- | --- |
| ELBSecurityPolítica-FS-2018-06 | • ECDHE-ECDSA- -GCM- AES128 SHA256<br>• ECDHE-RSA- AES128 -GCM- SHA256<br>• ECDHE-ECDSA- AES128 - SHA256<br>• ECDHE-RSA- - AES128 SHA256<br>• ECDHE-ECDSA- AES128 -SHA<br>• ECDHE-RSA- -SHA AES128<br>• ECDHE-ECDSA- AES256 -GCM- SHA384<br>• ECDHE-RSA- AES256 -GCM- SHA384<br>• ECDHE-ECDSA- AES256 - SHA384<br>• ECDHE-RSA- - AES256 SHA384<br>• ECDHE-RSA- AES256 -SHA<br>• ECDHE-ECDSA- AES256 -SHA |

## Políticas por cifrado

En la siguiente tabla se detallan las políticas de seguridad FS admitidas que admiten cada cifrado.

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
| --- | --- | --- |
| OpenSSL — 128-GCM - ECDHE-ECDSA-AES SHA256<br><br>IANA — TLS_ECDHE_ECDSA_CON_AES_128_GCM_ SHA256 | • ELBSecurityPolítica-FS-1-2-RES-2020-10<br>• ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c02b |
| OpenSSL — 128-GCM - ECDHE-RSA-AES SHA256 | • ELBSecurityPolítica-FS-1-2-RES-2020-10 | c02f |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
|---|---|---|
| IANA — TLS_ECDHE_RSA_CON_ AES_128_GCM_ SHA256 | • ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | |
| OpenSSL — 128- ECDHE-ECDSA-AES SHA256<br><br>IANA — TLS_ECDHE_ECDSA_CO N_AES_128_CBC_ SHA256 | • ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c023 |
| OpenSSL — 128- ECDHE-RSA-AES SHA256<br><br>IANA — TLS_ECDHE_RSA_CON_ AES_128_CBC_ SHA256 | • ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c027 |
| ECDHE-ECDSA-AESOpenSSL: 128-SHA<br><br>IANA: TLS_ECDHE_ECDSA_WI TH_AES_128_CBC_SHA | • ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c009 |
| ECDHE-RSA-AESOpenSSL: 128-SHA<br><br>IANA: TLS_ECDHE_RSA_WITH _AES_128_CBC_SHA | • ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c013 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
|---|---|---|
| OpenSSL — 256-GCM - ECDHE-ECDSA-AES SHA384<br>IANA — TLS_ECDHE_ECDSA_CON_AES_256_GCM_ SHA384 | • ELBSecurityPolítica-FS-1-2-RES-2020-10<br>• ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c02c |
| OpenSSL — 256-GCM - ECDHE-RSA-AES SHA384<br>IANA — TLS_ECDHE_RSA_CON_AES_256_GCM_ SHA384 | • ELBSecurityPolítica-FS-1-2-RES-2020-10<br>• ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c030 |
| OpenSSL — 256- ECDHE-ECDSA-AES SHA384<br>IANA — TLS_ECDHE_ECDSA_CON_AES_256_CBC_ SHA384 | • ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c024 |
| OpenSSL — 256- ECDHE-RSA-AES SHA384<br>IANA — TLS_ECDHE_RSA_CON_AES_256_CBC_ SHA384 | • ELBSecurityPolítica-FS-1-2-RES-2019-08<br>• ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c028 |

| Nombre del cifrado | Políticas de seguridad | Conjunto de cifrado |
|---|---|---|
| ECDHE-ECDSA-AESOpenSSL: 256-SHA<br><br>IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | • ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c00a |
| ECDHE-RSA-AESOpenSSL: 256-SHA<br><br>IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | • ELBSecurityPolítica-FS-1-2-2019-08<br>• ELBSecurityPolítica-FS-1-1-2019-08<br>• ELBSecurityPolítica-FS-2018-06 | c014 |

# Crear un oyente HTTPS para el equilibrador de carga de aplicaciones

Un oyente verifica solicitudes de conexión. Los oyentes se definen cuando se crea el equilibrador de carga, pero se pueden agregar otros oyentes en cualquier momento.

Para crear un oyente de HTTPS, debe implementar al menos un certificado de servidor SSL en el equilibrador de carga. El equilibrador de carga utiliza un certificado de servidor para terminar la conexión frontend y descifrar las solicitudes de los clientes antes de enviarlas a los destinos. Debe especificar también la política de seguridad que se utiliza para negociar las conexiones seguras entre los clientes y el equilibrador de carga.

Si necesita pasar tráfico cifrado a los destinos sin que el equilibrador de carga lo descifre, se puede crear un Equilibrador de carga de red o un Equilibrador de carga clásico con un oyente TCP en el puerto 443. Con un oyente TCP, el equilibrador de carga transfiere el tráfico cifrado a los destinos sin descifrarlo.

La información de esta página le ayuda a crear un oyente HTTPS para su equilibrador de carga. Para agregar un oyente HTTPS a un equilibrador de carga, consulte Crear un oyente HTTP para su equilibrador de carga de aplicaciones.

## Requisitos previos

- Para crear un oyente HTTPS, debe especificar un certificado y una política de seguridad. El equilibrador de carga usará el certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de direccionarlas a los destinos. El equilibrador de carga utiliza la política de seguridad para negociar conexiones SSL con los clientes.

  Los balanceadores de carga de aplicaciones no admiten claves. ED25519
- Para añadir una acción de reenvío a la regla predeterminada del oyente, debe especificar un grupo de destino disponible. Para obtener más información, consulte Creación de un grupo de destino para el Equilibrador de carga de aplicación.
- Puede especificar el mismo grupo de destino en varios oyentes, pero estos deben pertenecer al mismo equilibrador de carga. Para usar un grupo de destino con un equilibrador de carga, debe comprobar que un oyente no lo use para ningún otro equilibrador de carga.

## Agregar un oyente HTTPS

Los oyentes se configuran con un protocolo y un puerto para las conexiones entre los clientes y el equilibrador de carga, así como un grupo de destino para la regla predeterminada del oyente. Para obtener más información, consulte Configuración del oyente.

Cómo agregar un oyente HTTPS mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, seleccione Añadir oyente.
5. En Protocolo: puerto, elija HTTP y mantenga el puerto predeterminado o introduzca un puerto distinto.
6. (Opcional) Para activar la autenticación, en Autenticación, seleccione Usar OpenID o Amazon Cognito y proporcione la información solicitada. Para obtener más información, consulte Autenticación de usuarios mediante un Equilibrador de carga de aplicación.
7. Para las acciones de enrutamiento, realice una de las siguientes acciones:

   - Reenviar a los grupos de destino: elija los grupos de destino a los que desea reenviar el tráfico. Para añadir grupos de destino, seleccione Añadir grupo de destino. Si utiliza más

de un grupo de destino, seleccione una ponderación para cada uno y revise el porcentaje asociado. Debe habilitar la persistencia a nivel de grupo en una regla, si se activó la persistencia en uno o más de los grupos de destino.

- Redirigir a la URL: introduzca la URL a la que se redirigirán las solicitudes del cliente. Esto se puede hacer al introducir cada parte por separado en la pestaña partes de la URI o al ingrsear la dirección completa en la pestaña URL completa. Puede configurar las acciones de redirección como temporales (HTTP 302) o permanentes (HTTP 301), en función de sus necesidades para Código de estado.
- Devolver una respuesta fija: introduce el código de respuesta para volver a las solicitudes de los clientes rechazadas. Si lo desea, puede especificar el tipo de contenido y el cuerpo de la respuesta.

8. Para la política de seguridad, se recomienda utilizar siempre la política de seguridad predefinida más reciente.
9. En SSL/TLS Certificado predeterminado, elija el certificado predeterminado. También agregamos el certificado predeterminado a la lista de SNI. Puede seleccionar el certificado de una de las siguientes fuentes:

   - Si creó o importó un certificado utilizando AWS Certificate Manager, seleccione De ACM y, a continuación, elija el certificado de Certificado (de ACM).
   - Si ha importado un certificado mediante IAM, seleccione De IAM y, a continuación, elija el certificado de Certificado (de IAM).
   - Si tiene un certificado, elija Importar certificado. Elija Importar a ACM o Importar a IAM. En el caso de la clave privada del certificado, copie y pegue el contenido del archivo de clave privada (codificado en PEM). Para el cuerpo del certificado, copie y pegue el contenido del archivo de certificado de clave pública (codificado en PEM). En el caso de la cadena de certificados, copie y pegue el contenido del archivo de la cadena de certificados (codificado en PEM), a menos que utilice un certificado autofirmado y no sea importante que los navegadores acepten implícitamente el certificado.

10. (Opcional) Para habilitar la autenticación mutua, en Gestión de certificados de cliente, habilite la autenticación mutua (mTLS).

    Cuando está activado, el modo TLS mutuo predeterminado es de acceso directo.

    Si selecciona Verificar con el almacén de confianza:

- De forma predeterminada, se rechazan las conexiones con certificados de cliente vencidos. Para cambiar este comportamiento, abra la configuración avanzada de mTLS y, en Caducidad del certificado de cliente, seleccione Permitir certificados de cliente caducados.
- En Almacén de confianza, seleccione un almacén de confianza existente o elija Nuevo almacén de confianza.
  - Si ha elegido un nuevo almacén de confianza, proporcione un nombre de almacén de confianza, la ubicación de la entidad de certificación URI S3 y, si lo desea, una ubicación en la lista de revocaciones de certificados URI S3.
- (Opcional) Seleccione si desea activar los nombres de asunto de Anuncie TrustStore CA.

11. Elija Agregar.
12. Para añadir certificados a la lista de certificados opcionales, consulteAñadir certificados a la lista de certificados.

Para añadir un agente de escucha HTTPS mediante el AWS CLI

Utilice el comando create-oyente para crear el oyente y la regla predeterminada, y el comando create-rule para definir nuevas reglas del oyente.

# Reglas del oyente del equilibrador de carga de aplicaciones

Las reglas que se definen para el oyente determinan cómo el equilibrador 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 más acciones y una o más condiciones. Para obtener más información, consulte Reglas del oyente.

## 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 para el Equilibrador de carga de aplicación.

## Agregar una regla

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

Para agregar una regla a través de la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga para ver sus detalles.
4. En la pestaña Oyentes y reglas, realice alguna de las siguientes acciones:

   a. Seleccione el texto de la columna Protocol:Port para abrir la página de detalles del oyente.

      En la pestaña Reglas, seleccione Añadir regla.

   b. Seleccione el oyente al que desea agregar una regla.

      Seleccione Administrar reglas y, a continuación, Agregar regla.
5. Puede especificar un nombre para la regla en Nombre y etiquetas, aunque no es obligatorio.

   Para agregar otras etiquetas, elija Agregar etiqueta adicional.
6. Elija Siguiente.
7. Elija Add condition.
8. Añada una o varias de las siguientes condiciones:

   - Encabezado de host: defina el encabezado de host. Por ejemplo: `*.example.com`. Elija Confirmar para guardar la condición.

     128 caracteres como máximo. No distingue entre mayúsculas y minúsculas. Los caracteres permitidos son a-z, 0-9; los siguientes caracteres especiales: -_.; y caracteres comodín (* y?). Debe incluir al menos un carácter “.”. Solo puede contener caracteres alfabéticos detrás del carácter “.” final.
   - Ruta: defina la ruta. Por ejemplo: `/item/*` . Elija Confirmar para guardar la condición.

128 caracteres como máximo. Distingue mayúsculas de minúsculas. Los caracteres permitidos son letras a-z, A-Z, números 0-9; los siguientes caracteres especiales: _-.$/~'"@; &; y caracteres comodín (* y ?).

- Método de solicitud HTTP: defina el método de solicitud HTTP. Elija Confirmar para guardar la condición.

  40 caracteres como máximo. Distingue mayúsculas de minúsculas. Los caracteres permitidos son letras A-Z y los siguientes caracteres especiales: -_. No se admite el uso de comodines.

- IP de origen: defina la dirección IP de origen en formato CIDR. Elija Confirmar para guardar la condición.

  Ambos IPv4 IPv6 CIDRs están permitidos. No se admite el uso de comodines.

- Encabezado HTTP: escriba el nombre del encabezado y añada una o varias cadenas de comparación. Elija Confirmar para guardar la condición.
  - Nombre del encabezado HTTP: la regla evaluará las solicitudes que contengan este encabezado para confirmar los valores coincidentes.

    40 caracteres como máximo. No distingue entre mayúsculas y minúsculas. Los caracteres permitidos son letras de la a-z, A-Z, números 0-9 y los siguientes caracteres especiales: *? -! #$%&'+.^_`|~. No se admite el uso de comodines.
  - Valor de encabezado HTTP: ingrese cadenas que se van a comparar con el valor del encabezado HTTP.

    128 caracteres como máximo. No distingue entre mayúsculas y minúsculas. Los caracteres permitidos son a-z, A-Z, 0-9; espacios; los siguientes caracteres especiales:!» #$%&' () +,. /:; <=>@ [] ^_` {|} ~-; y caracteres comodín (* y?).
- Cadena de consulta: enruta las solicitudes en función de pares clave/valor o en valores en las cadenas de consulta. Elija Confirmar para guardar la condición.

  128 caracteres como máximo. No distingue entre mayúsculas y minúsculas. Los caracteres permitidos son letras a-z, AZ, números 0-9; los siguientes caracteres especiales: _-.$/~'"@: +&()!,;=; y caracteres comodín (* y ?).

9. Elija Siguiente.
10. Defina una de las siguientes acciones para la regla:

- Reenviar a los grupos de destino: elija uno o más grupos de destino a los que reenviar el tráfico. Para añadir grupos de destino, seleccione Añadir grupo de destino. Si utiliza más de un grupo de destino, seleccione una ponderación para cada uno y revise el porcentaje asociado. Debe habilitar la persistencia a nivel de grupo en una regla, si se activó la persistencia en uno o más de los grupos de destino.
- Redirigir a la URL: especifique la URL a la que se redirigirán las solicitudes de los clientes. Esto se puede hacer al introducir cada parte por separado en la pestaña partes de la URI o al ingrsear la dirección completa en la pestaña URL completa. Puede configurar las acciones de redirección como temporales (HTTP 302) o permanentes (HTTP 301), en función de sus necesidades para Código de estado.
- Devolver una respuesta fija: especifique el código de respuesta que se devolverá a las solicitudes de los clientes rechazadas. Además, puede especificar el tipo de contenido y el cuerpo de la respuesta, pero no son obligatorios.

11. Elija Siguiente.
12. Especifique la prioridad de la regla; para ello, introduzca un valor comprendido entre 1 y 50 000.
13. Elija Siguiente.
14. Revise todos los detalles y los ajustes configurados actualmente para la nueva regla. Una vez que esté satisfecho con la configuración, seleccione Crear.

Para añadir una regla mediante el 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. Las actualizaciones de reglas no tienen efecto inmediatamente, por lo que las solicitudes pueden direccionarse utilizando la configuración de reglas anterior durante un breve periodo de tiempo después de actualizar una regla. Todas las solicitudes en tránsito están completadas.

Para editar una regla a través de la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.

4. En la pestaña Oyentes y reglas, realice alguna de las siguientes acciones:

   - Seleccione el texto de la columna Protocolp:Puerto para abrir la página de detalles del oyente.

     i. En la pestaña Reglas, en la sección Reglas de oyente, seleccione el texto de la columna Etiqueta de nombre para la regla que desee editar.

        Elija Acciones y, a continuación, Editar.

     ii. En la pestaña Reglas, en la sección Reglas de oyente, seleccione la regla que desee editar.

         Elija Acciones y, a continuación, Editar.

5. Modifique el nombre y las etiquetas según sea necesario. Para agregar otras etiquetas, elija Agregar etiqueta adicional.
6. Elija Siguiente.
7. Modifique las condiciones según sea necesario. Puede agregar, editar una condición existente o eliminar las condiciones.
8. Elija Siguiente.
9. Modifique las acciones según sea necesario.
10. Elija Siguiente.
11. Modifique la prioridad de la regla según sea necesario. Puede introducir un valor entre 1 y 50 000.
12. Elija Siguiente.
13. Revise todos los detalles y los ajustes actualizados que haya configurado en la nueva regla. Cuando las selecciones le parezcan adecuadas, seleccione Guardar cambios.

Para editar una regla mediante el AWS CLI

Utilice el comando modify-rule.

## Actualizar la prioridad de una regla

Las reglas 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.

Actualización de la prioridad de la regla a través de la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, realice alguna de las siguientes acciones:
   a. Seleccione el texto de las columnas Protocol:Port o Reglas para abrir la página de detalles del oyente.
      i. Seleccione Acciones y, a continuación, Volver a priorizar las reglas.
      ii. En la pestaña Reglas, en la sección Reglas de oyente, seleccione Acciones y, a continuación, Cambiar la prioridad de las reglas.
   b. Seleccionar el oyente.
      • Seleccione Administrar reglas y, a continuación, Cambiar la prioridad de las reglas
5. En la sección Reglas de oyente, la columna Prioridad muestra la prioridad de las reglas actuales. Puede actualizar la prioridad de las reglas introduciendo un valor comprendido entre 1 y 50 000.
6. Cuando los cambios le parezcan finalizados, seleccione Guardar cambios.

Para actualizar las prioridades de las reglas mediante el AWS CLI

Utilice el comando set-rule-priorities.

## Eliminar una regla

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

Para eliminar una regla a través de la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, realice alguna de las siguientes acciones:

a. Seleccione el texto de las columnas Protocolo:Puerto o Reglas para abrir la página de detalles del oyente.

   i. Seleccione la regla que desea eliminar.

   ii. Seleccione Acciones, y luego Eliminar regla.

   iii. Escriba `confirm` en el campo de texto y elija Eliminar.

b. Seleccione el texto de la columna Etiqueta de nombre para abrir la página de detalles de la regla.

   i. Seleccione Acciones, y luego Eliminar regla.

   ii. Escriba `confirm` en el campo de texto y elija Eliminar.

Para eliminar una regla, usa el AWS CLI

Utilice el comando delete-rule.

# Actualizar un oyente HTTPS para el equilibrador de carga de aplicaciones

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

Tareas

- Reemplazar el certificado predeterminado
- Añadir certificados a la lista de certificados
- Quitar certificados de la lista de certificados
- Actualizar la política de seguridad
- Modificación del encabezado HTTP

## Reemplazar el certificado predeterminado

Puede reemplazar el certificado predeterminado para su oyente utilizando el siguiente procedimiento. Para obtener más información, consulte Certificados SSL para el Equilibrador de carga de aplicación.

Para reemplazar el certificado predeterminado a través de la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, elija el texto de la columna Protocolo:Puerto para abrir la página de detalles del oyente.
5. En la pestaña Certificados, elija Cambiar el valor predeterminado.
6. En la tabla de certificados de ACM e IAM, seleccione un nuevo certificado predeterminado.
7. Seleccione Guardar como predeterminado.

Para reemplazar el certificado predeterminado mediante el AWS CLI

Utilice el comando modify-oyente.

## Añadir certificados a la lista de certificados

Puede añadir certificados a la lista de certificados para su oyente utilizando el siguiente procedimiento. Si creó el listener con el AWS Management Console, agregamos el certificado predeterminado a la lista de certificados por usted. De lo contrario, la lista de certificados está vacía. Al agregar el certificado predeterminado a la lista de certificados, se garantiza que este certificado se utilice con el protocolo SNI aunque se sustituya como certificado predeterminado. Para obtener más información, consulte Certificados SSL para el Equilibrador de carga de aplicación.

Para añadir certificados a la lista de certificados utilizando la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, elija el texto de la columna Protocolo:Puerto para abrir la página de detalles del oyente.
5. En la pestaña Certificados, elija Agregar certificado.
6. Para añadir certificados que ya están gestionados por ACM o IAM, seleccione las casillas de verificación de los certificados y, a continuación, seleccione Incluir como pendientes, que aparece a continuación.

7. Si cuenta con un certificado que no se encuentra administrado por ACM o IAM, elija Importar certificado, complete el formulario y elija Importar.
8. Elija Agregar certificados pendientes.

Para añadir un certificado a la lista de certificados mediante 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 oyente HTTPS utilizando el siguiente procedimiento. Tras eliminar un certificado, el oyente ya no podrá crear conexiones con ese certificado. Para garantizar que los clientes no se vean afectados, añada un certificado nuevo a la lista y confirme que las conexiones funcionan antes de eliminar un certificado de la lista.

Para quitar el certificado predeterminado de un agente de escucha TLS, consulte Reemplazar el certificado predeterminado.

Para quitar certificados de la lista de certificados utilizando la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Listeners and rules, seleccione el texto de la columna Protocol:Port para abrir la página de detalles del oyente.
5. En la pestaña Certificados, seleccione la casillas de los certificados y elija Eliminar.
6. Cuando se le solicite confirmación, ingrese **`confirm`** y elija Eliminar.

Para eliminar un certificado de la lista de certificados mediante el AWS CLI

Utilice el comando remove-listener-certificates.

## Actualizar la política de seguridad

Cuando crea un oyente 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 oyente HTTPS para que la utilice. Los equilibradores de carga de aplicaciones no admiten políticas de

seguridad personalizadas. Para obtener más información, consulte Políticas de seguridad para el Equilibrador de carga de aplicación.

La actualización de la política de seguridad puede provocar interrupciones si el equilibrador de cargas gestiona un gran volumen de tráfico. Para reducir la posibilidad de interrupciones cuando el balanceador de cargas gestiona un gran volumen de tráfico, crea un balanceador de carga adicional que ayude a gestionar el tráfico o solicita una reserva de LCU.

Uso de políticas de FIPS en su Application Load Balancer

Todos los oyentes seguros conectados a un Equilibrador de carga de aplicación deben usar políticas de seguridad FIPS o políticas de seguridad que no sean FIPS; recuerde que no se pueden mezclar. Si un Equilibrador de carga de aplicación existente tiene dos o más oyentes que utilizan políticas que no son FIPS y desea que los oyentes usen políticas de seguridad FIPS en su lugar, elimine todos los oyentes hasta que solo quede uno. Cambie la política de seguridad del oyente a FIPS y, a continuación, cree más oyentes mediante las políticas de seguridad de FIPS. Como alternativa, puede crear un nuevo Equilibrador de carga de aplicación con nuevos oyentes utilizando únicamente las políticas de seguridad FIPS.

Para actualizar la política de seguridad a través de la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, elija el texto de la columna Protocolo:Puerto para abrir la página de detalles del oyente.
5. A continuación, en la página Detalles, elija Acciones, y luego Editar oyente.
6. En la sección Configuración segura del oyente, en Política de seguridad, elija una nueva política de seguridad.
7. Seleccione Save changes (Guardar cambios).

Para actualizar la política de seguridad mediante el AWS CLI

Utilice el comando modify-oyente.

## Modificación del encabezado HTTP

La modificación del encabezado HTTP te permite cambiar el nombre de encabezados específicos generados por el balanceador de cargas, insertar encabezados de respuesta específicos y deshabilitar el encabezado de respuesta del servidor. Los balanceadores de carga de aplicaciones admiten la modificación de encabezados tanto para los encabezados de solicitud como para los de respuesta.

Para obtener más información, consulte Habilite la modificación del encabezado HTTP para su Application Load Balancer.

# Autenticación mutua con TLS en Equilibrador de carga de aplicación

La autenticación TLS mutua es una variación de la seguridad de la capa de transporte (TLS). La TLS tradicional establece comunicaciones seguras entre un servidor y un cliente, donde el servidor debe proporcionar su identidad a sus clientes. Con la TLS mutua, un equilibrador de carga negocia la autenticación mutua entre el cliente y el servidor mientras negocia TLS. Al usar la TLS mutua con el Equilibrador de carga de aplicación, se simplifica la administración de la autenticación y se reduce la carga de las aplicaciones.

Al usar la TLS mutua con el Equilibrador de carga de aplicación, su equilibrador de carga puede administrar la autenticación de los clientes para garantizar que solo los clientes de confianza se comuniquen con sus aplicaciones de backend. Al utilizar esta función, Application Load Balancer autentica a los clientes con certificados de una entidad emisora de certificados (CA) externa o mediante la AWS Private Certificate Authority (PCA), de forma opcional, con comprobaciones de revocación. Equilibrador de carga de aplicación transmite la información del certificado del cliente al backend, que las aplicaciones pueden utilizar para la autorización. Al usar la TLS mutua en Equilibrador de carga de aplicación, puede obtener una autenticación integrada, escalable y administrada para las entidades basadas en certificados, que utilizan bibliotecas establecidas.

La TLS mutua para los Equilibradores de carga de aplicación ofrece las dos opciones siguientes para validar los certificados de cliente X.509v3:

Nota: No se admiten los certificados de cliente X.509v1.

- Acceso directo a TLS mutua: cuando se utiliza el modo de acceso directo a TLS mutua, el Equilibrador de carga de aplicación envía toda la cadena de certificados del cliente al destino

mediante encabezados HTTP. Luego, si usa la cadena de certificados del cliente, puede implementar la correspondiente autenticación del equilibrador de carga y la lógica de autorización de destino en su aplicación.

- Verificación TLS mutua: cuando se usa el modo de verificación TLS mutua, Equilibrador de carga de aplicación realiza la autenticación del certificado de cliente X.509 para los clientes cuando un equilibrador de carga negocia las conexiones de TLS.

Para empezar a utilizar la TLS mutua en Equilibrador de carga de aplicación mediante el acceso directo, solo tiene que configurar al oyente para que acepte los certificados de los clientes. Para utilizar la TLS mutua con procesos de verificación, debe hacer lo siguiente:

- Cree un nuevo recurso del almacén de confianza.
- Cargue su paquete de entidades de certificación (CA) y, si lo desea, las listas de revocación.
- Adjunte el almacén de confianza al oyente que está configurado para verificar los certificados de los clientes.

Para conocer step-by-step los procedimientos para configurar el modo de verificación TLS mutua con su Application Load Balancer, consulte. Configuración de una TLS mutua en un Equilibrador de carga de aplicación

## Pasos previos a la configuración de la TLS mutua en el Equilibrador de carga de aplicación

Antes de empezar a configurar la TLS mutua en el Equilibrador de carga de aplicación, tenga en cuenta lo siguiente:

Cuotas

Los balanceadores de carga de aplicaciones incluyen ciertos límites relacionados con la cantidad de almacenes de confianza, certificados de CA y listas de revocación de certificados que se utilizan en su cuenta. AWS

Para obtener más información, consulte Cuotas para sus Equilibradores de carga de aplicación.

Requisitos para certificados

Los Equilibradores de carga de aplicación son compatibles con los siguientes elementos para los certificados que se utilizan con la autenticación TLS mutua:

- Certificado compatible: X.509v3
- Claves públicas compatibles: RSA 2K — 8K o ECDSA secp256r1, secp384r1, secp521r1
- Algoritmos de firma compatibles: 384 SHA256, 512 con RSA/SHA256, 384, 512 with EC/SHA 256 384 512 hash con RSASSA-PSS con MGF1

Agrupaciones de certificados de CA

La siguiente información se aplica a los paquetes de entidades de certificación (CA):

- Los Equilibradores de carga de aplicación cargan cada paquete de certificados de la entidad de certificación (CA) en un lote. Los Equilibradores de carga de aplicación no admiten la carga de certificados individuales. Si necesita agregar nuevos certificados, debe cargar el archivo del paquete de certificados.
- Para reemplazar un paquete de certificados de CA, utilice la API. ModifyTrustStore

Solicitud de certificado para acceso directo

Cuando se utiliza el acceso directo de TLS mutua, el Equilibrador de carga de aplicación inserta encabezados para presentar la cadena de certificados del cliente a los destinos del backend. El orden de presentación comienza con los certificados de hoja y termina con el certificado raíz.

Reanudación de la sesión

No se admite la reanudación de la sesión cuando se utilizan los modos de verificación o los accesos directos de TLS mutua con un Equilibrador de carga de aplicación.

Encabezados HTTP

Los Equilibradores de carga de aplicación utilizan encabezados `X-Amzn-Mtls` para enviar la información del certificado cuando negocian las conexiones de los clientes mediante una TLS mutua. Para obtener más información y ejemplos, consulte Encabezados HTTP y TLS mutua.

Archivos de certificados de CA

Tenga en cuenta que los certificados de CA deben satisfacer los siguientes requisitos:

- El archivo de certificado debe usar el formato PEM (Privacy Enhanced Mail).
- El contenido del certificado debe estar dentro de los límites `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----`.
- Los comentarios deben ir precedidos de un carácter # y no deben contener ningún carácter `-`.
- No puede haber líneas en blanco.

Ejemplo de un certificado que no se acepta (no válido):

```
# comments

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 01
    Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=US, O=EXAMPLE, OU=EXAMPLE, CN=EXAMPLE
        Validity
            Not Before: Jan 11 23:57:57 2024 GMT
            Not After : Jan 10 00:57:57 2029 GMT
        Subject: C=US, O=EXAMPLE, OU=EXAMPLE, CN=EXAMPLE
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    00:01:02:03:04:05:06:07:08
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                00:01:02:03:04:05:06:07:08
            X509v3 Subject Alternative Name:
                URI:EXAMPLE.COM
    Signature Algorithm: ecdsa-with-SHA384
         00:01:02:03:04:05:06:07:08
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

Ejemplos de certificados que se aceptan (válidos):

1. Certificado único (codificado en PEM):

```
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

2. Varios certificados (codificados en PEM):

```
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
# comments
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Base64-encoded certificate
-----END CERTIFICATE-----
```

## Encabezados HTTP y TLS mutua

En esta sección, se describen los encabezados HTTP que los Equilibradores de carga de aplicación utilizan para enviar la información de los certificados cuando negocian conexiones con clientes que utilizan una TLS mutua. Los encabezados `X-Amzn-Mtls` específicos que utiliza el Equilibrador de carga de aplicación dependen del modo de TLS mutua que haya especificado: modo de acceso directo o modo de verificación.

Para obtener información sobre otros encabezados HTTP compatibles con los Equilibradores de carga de aplicación, consulte Encabezados HTTP y balanceadores de tipo equilibrador de carga de aplicaciones.

### Encabezado de HTTP para el modo de acceso directo

Para la TLS mutua en modo de acceso directo, los Equilibradores de carga de aplicación utilizan el siguiente encabezado.

X-Aman-Mtls-Clientcert

Este encabezado contiene el formato PEM codificado en una URL de toda la cadena de certificados de cliente presentada en la conexión, con los caracteres seguros `+=/`.

Ejemplo de contenido del encabezado:

```
X-Amzn-Mtls-Clientcert: -----BEGIN%20CERTIFICATE-----%0AMIID<...reduced...>do0g
%3D%3D%0A-----END%20CERTIFICATE-----%0A-----BEGIN%20CERTIFICATE-----
%0AMIID1<...reduced...>3eZlyKA%3D%3D%0A-----END%20CERTIFICATE-----%0A
```

## Encabezados de HTTP para el modo de verificación

Para la TLS mutua en modo de verificación, los Equilibradores de carga de aplicación utilizan los siguientes encabezados.

X-Amzn-Mtls-Clientcert-Serial-Number

Este encabezado contiene una representación hexadecimal del número de serie del certificado de hoja.

Ejemplo de contenido del encabezado:

```
X-Amzn-Mtls-Clientcert-Serial-Number: 03A5B1
```

X-Amzn-Mtls-Clientcert-Issuer

Este encabezado contiene una RFC2253 cadena que representa el nombre distintivo (DN) del emisor.

Ejemplo de contenido del encabezado:

```
X-Amzn-Mtls-Clientcert-Issuer:
 CN=rootcamtls.com,OU=rootCA,O=mTLS,L=Seattle,ST=Washington,C=US
```

X-Amzn-Mtls-Clientcert-Subject

Este encabezado contiene una representación en RFC2253 cadena del nombre distintivo (DN) del sujeto.

Ejemplo de contenido del encabezado:

```
X-Amzn-Mtls-Clientcert-Subject: CN=client_.com,OU=client-3,O=mTLS,ST=Washington,C=US
```

X-Amzn-Mtls-Clientcert-Validity

Este encabezado contiene un formato ISO86 01 de la `notAfter` fecha `notBefore` y.

Ejemplo de contenido del encabezado:

```
X-Amzn-Mtls-Clientcert-Validity:
 NotBefore=2023-09-21T01:50:17Z;NotAfter=2024-09-20T01:50:17Z
```

X-Amzn-Mtls-Clientcert-Leaf

Este encabezado contiene un formato PEM codificado en una dirección URL del certificado de hoja, con los caracteres seguros `+=/`.

Ejemplo de contenido del encabezado:

```
X-Amzn-Mtls-Clientcert-Leaf: -----BEGIN%20CERTIFICATE-----%0AMIIG<...reduced...>NmrUlw
%0A-----END%20CERTIFICATE-----%0A
```

## Anuncie el nombre del asunto de la autoridad de certificación (CA)

Los nombres de asunto de Advertising Certificate Authority (CA) mejoran el proceso de autenticación al ayudar a los clientes a determinar qué certificados se aceptarán durante la autenticación TLS mutua.

Al activar Anunciar los nombres de asunto de CA, Application Load Balancer anunciará la lista de nombres de asunto de las autoridades de certificación (CAs) en las que confía, en función del almacén de confianza al que esté asociado. Cuando un cliente se conecta a un destino a través del Application Load Balancer, el cliente recibe la lista de nombres de sujetos de CA de confianza.

Durante el protocolo de enlace TLS, cuando Application Load Balancer solicita un certificado de cliente, incluye una lista de nombres distinguidos de CA de confianza DNs () en su mensaje de solicitud de certificado. Esto ayuda a los clientes a seleccionar certificados válidos que coincidan con los nombres de asunto de las entidades de certificación anunciadas, lo que agiliza el proceso de autenticación y reduce los errores de conexión.

Puede activar Anunciar el nombre del asunto de CA en los oyentes nuevos y existentes. Para obtener más información, consulte Agregar un oyente HTTPS.

## Registros de conexión de Equilibradores de carga de aplicación

Elastic Load Balancing proporciona registros de conexión que capturan atributos sobre las solicitudes enviadas a los Equilibradores de carga de aplicación. Los registros de conexión contienen

información como la dirección IP y el puerto del cliente, la información del certificado del cliente, los resultados de la conexión y los cifrados TLS que se utilizan. Estos registros de conexión se pueden usar luego para revisar los patrones de solicitudes y otras tendencias.

Para obtener más información sobre los registros de conexión, consulte Registros de conexión del Equilibrador de carga de aplicación.

## Configuración de una TLS mutua en un Equilibrador de carga de aplicación

Esta sección incluye los procedimientos para configurar el modo de verificación de una TLS mutua para la autenticación en los Equilibradores de carga de aplicación.

Para utilizar el modo de acceso directo de la TLS mutua, solo tiene que configurar al oyente para que acepte los certificados de los clientes. Cuando utiliza el acceso directo de TLS mutua, el Equilibrador de carga de aplicación envía toda la cadena de certificados del cliente al destino mediante encabezados de HTTP, lo que le permite implementar la lógica de autenticación y autorización correspondiente en la aplicación. Para obtener más información, consulte Crear un oyente HTTPS para el Equilibrador de carga de aplicaciones.

Cuando se usa la TLS mutua en el modo de verificación, el Equilibrador de carga de aplicación realiza la autenticación del certificado de cliente X.509 para los clientes cuando un equilibrador de carga negocia las conexiones de TLS.

Para usar el modo de verificación de TLS mutua, realice lo siguiente:

- Cree un nuevo recurso del almacén de confianza.
- Cargue su paquete de entidades de certificación (CA) y, si lo desea, las listas de revocación.
- Adjunte el almacén de confianza al oyente que está configurado para verificar los certificados de los clientes.

Siga los procedimientos de esta sección para configurar el modo de verificación de TLS mutua en su Equilibrador de carga de aplicación en AWS Management Console. Para configurar la TLS mutua mediante operaciones de API en lugar de la consola, consulte la Guía de referencia de la API del Equilibrador de carga de aplicación.

Tareas

- Creación de un almacén de confianza
- Asociar un almacén de confianza

- Consulta de los detalles del almacén de confianza
- Modificación de un almacén de confianza
- Eliminación de un almacén de confianza

## Creación de un almacén de confianza

Hay tres formas de crear un almacén de confianza: al crear un Equilibrador de carga de aplicación, al crear un oyente seguro y mediante la consola del almacén de confianza. Al agregar un almacén de confianza al crear un equilibrador de carga o un oyente, el almacén de confianza se asocia automáticamente al nuevo oyente. Al crear un almacén de confianza mediante la consola del almacén de confianza, debe asociarlo a un oyente.

En esta sección se describe la creación de un almacén de confianza mediante la consola del almacén de confianza, pero los pasos que se siguen al crear un Equilibrador de carga de aplicación o un oyente son los mismos. Para obtener más información, consulte Configurar un equilibrador de carga y un oyente y Crear un oyente de HTTPS.

Requisitos previos:

- Para crear un almacén de confianza, debe tener un paquete de certificados de su entidad de certificación (CA).

Creación de un almacén de confianza mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, seleccione Almacenes de confianza.
3. Seleccione Crear un almacén de confianza.
4. Configuración del almacén de confianza
   a. En Nombre del almacén de confianza, introduzca un nombre para este.
   b. En el paquete de la entidad de certificación, introduzca la ruta de Amazon S3 al paquete de certificados de CA que desee que utilice su almacén de confianza.

      Opcional: utilice la versión de objeto para seleccionar una versión anterior del paquete de certificados de CA. De lo contrario, se utilizará la versión actual.
5. En el caso de las revocaciones, si lo desea, puede agregar una lista de revocación de certificados a su almacén de confianza.

- En Lista de revocación de certificados, introduzca la ruta de Amazon S3 en la lista de revocación de certificados que quiera que utilice su almacén de confianza.

  Opcional: utilice la versión de objeto para seleccionar una versión anterior de la lista de revocación de certificados. De lo contrario, se utilizará la versión actual.

6. En el caso de las etiquetas del almacén de confianza, si lo desea, puede introducir hasta 50 etiquetas para aplicarlas a su almacén de confianza.
7. Seleccione Crear un almacén de confianza.

## Asociar un almacén de confianza

Tras crear un almacén de confianza, debe asociarlo a un oyente para que el Equilibrador de carga de aplicación pueda empezar a utilizar el almacén de confianza. Recuerde que solo puede tener un almacén de confianza asociado a cada uno de sus oyentes seguros, pero un almacén de confianza puede estar asociado a varios oyentes.

En esta sección se describe la asociación de un almacén de confianza a un oyente existente. Como alternativa, puede asociar un almacén de confianza al crear un Equilibrador de carga de aplicación o un oyente. Para obtener más información, consulte Configurar un equilibrador de carga y un oyente y Crear un oyente de HTTPS.

Asociación de un almacén de confianza mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga para ver la página de detalles.
4. En la pestaña Oyentes y reglas, elija el enlace de la columna Protocol:Port para abrir la página de detalles del oyente seguro.
5. En la pestaña Seguridad, seleccione Editar la configuración del oyente seguro.
6. (Opcional) Si la TLS mutua no está habilitada, seleccione Autenticación mutua (mTLS) en Gestión de certificados de cliente y, a continuación, elija Verificar con el almacén de confianza.
7. En Almacén de confianza, elija el almacén de confianza que creó.
8. Seleccione Save changes (Guardar cambios).

## Consulta de los detalles del almacén de confianza

### Agrupaciones de certificados de CA

El paquete de certificados de CA es un componente obligatorio del almacén de confianza. Es un conjunto de certificados raíz e intermedios de confianza que ha validado una entidad de certificación. Estos certificados validados garantizan que el cliente pueda confiar en que el certificado que se presenta es propiedad del equilibrador de carga.

Puede ver el contenido del paquete de certificados de CA actual en su almacén de confianza en cualquier momento.

### Consulta de un paquete de certificados de CA

#### Consulta de un paquete de certificado de CA mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, seleccione Almacenes de confianza.
3. Seleccione el almacén de confianza para ver la página de detalles.
4. Seleccione Acciones y, a continuación, Obtener el paquete de CA.
5. Elija Compartir enlace o Descargar.

### Listas de revocación de certificados

Si lo desea, puede crear una lista de revocación de certificados para un almacén de confianza. Las autoridades de certificación publican las listas de revocación; estas últimas contienen datos de los certificados que se han revocado. Los Equilibradores de carga de aplicación solo admiten listas de revocación de certificados en formato PEM.

Cuando se agrega una lista de revocación de certificados a un almacén de confianza, se le asigna un identificador de revocación. La revocación IDs aumenta por cada lista de revocaciones que se añada al almacén de confianza y no se puede cambiar. Si se elimina una lista de revocación de certificados de un almacén de confianza, su ID de revocación también se elimina y no se reutiliza mientras funcione el almacén de confianza.

> **Note**
>
> Los Equilibradores de carga de aplicación no pueden revocar los certificados que tengan un número de serie negativo dentro de una lista de revocación de certificados.

Consulta de una lista de revocación de certificados

Consulta de una lista de revocaciones mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, seleccione Almacenes de confianza.
3. Seleccione el almacén de confianza para ver la página de detalles.
4. En la pestaña Listas de revocación de certificados, seleccione Acciones y, a continuación, Obtener lista de revocación.
5. Elija Compartir enlace o Descargar.

## Modificación de un almacén de confianza

Un almacén de confianza solo puede contener un paquete de certificados de CA a la vez, pero puede reemplazar el paquete de certificados de CA en cualquier momento una vez haya creado el almacén de confianza.

Sustitución de un paquete de certificados de CA

Sustitución de un paquete de certificados de CA mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, seleccione Almacenes de confianza.
3. Seleccione el almacén de confianza para ver la página de detalles.
4. Seleccione Acciones y, a continuación, Reemplazar el paquete de CA.
5. En la página Reemplazar el paquete de CA, en Paquete de entidades de certificación, introduzca la ubicación de Amazon S3 del paquete de CA deseado.
6. (Opcional) Utilice la versión de objeto para seleccionar una versión anterior de la lista de revocación de certificados. De lo contrario, se utilizará la versión actual.
7. Seleccione Reemplazar el paquete de CA.

### Incorporación de una lista de revocación de certificados

Incorporación de una lista de revocación mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, seleccione Almacenes de confianza.
3. Seleccione el almacén de confianza para ver su página de detalles.
4. En la pestaña Listas de revocación de certificados, seleccione Acciones y, a continuación, Agregar la lista de revocación.
5. En la página Agregar lista de revocación, en Lista de revocación de certificados, introduzca la ubicación de Amazon S3 de la lista de revocación de certificados que quiera.
6. (Opcional) Utilice la versión de objeto para seleccionar una versión anterior de la lista de revocación de certificados. De lo contrario, se utilizará la versión actual.
7. Seleccione Agregar lista de revocación

### Eliminación de una lista de revocación de certificados

Eliminación de una lista de revocación mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación izquierdo, seleccione Almacenes de confianza.
3. Seleccione el almacén de confianza para ver la página de detalles.
4. En la pestaña Listas de revocación de certificados, seleccione Acciones y, a continuación, Eliminar lista de revocación.
5. Para confirmar la eliminación, escriba `confirm`.
6. Seleccione Eliminar.

## Eliminación de un almacén de confianza

Cuando ya no utilice un almacén de confianza, puede eliminarlo.

Nota: No puede eliminar un almacén de confianza que esté actualmente asociado a un oyente.

Eliminación de un almacén de confianza mediante la consola

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

2. En el panel de navegación izquierdo, seleccione Almacenes de confianza.
3. Seleccione el almacén de confianza para ver su página de detalles.
4. Elija Acciones y, a continuación, Eliminar almacén de confianza.
5. Para confirmar la eliminación, escriba `confirm`.
6. Seleccione Eliminar.

## Cómo compartir el almacén de confianza de Elastic Load Balancing para los Equilibradores de carga de aplicación

Elastic Load Balancing se integra con AWS Resource Access Manager (AWS RAM) para permitir el uso compartido en almacenes de confianza. AWS RAM es un servicio que le permite compartir de forma segura los recursos de su almacén fiduciario de Elastic Load Balancing entre su organización o unidades organizativas Cuentas de AWS y dentro de ellas (OUs). Si tiene varias cuentas, puede crear un almacén de confianza una vez y usar AWS RAM para que otras cuentas puedan usarlo. Si su cuenta está gestionada por AWS Organizations, puede compartir los almacenes fiduciarios con todas las cuentas de la organización o solo con las cuentas de las unidades organizativas especificadas (OUs).

Con AWS RAM, compartes los recursos de tu propiedad mediante la creación de un recurso compartido. Un uso compartido de recursos especifica los recursos que compartir y los consumidores con quienes compartirlos. En este modelo, el Cuenta de AWS propietario del almacén fiduciario (propietario) lo comparte con otros Cuentas de AWS (consumidores). Los consumidores pueden asociar los almacenes de confianza compartidos a sus oyentes del Equilibrador de carga de aplicación del mismo modo que asocian los almacenes de confianza en su propia cuenta.

El propietario de un almacén de confianza puede compartir un almacén de confianza con:

- Cuentas de AWS Específico dentro o fuera de su organización en AWS Organizations
- Una unidad organizativa dentro de su organización en AWS Organizations
- Toda su organización en AWS Organizations

Contenido

- Cómo compartir un almacén de confianza
- Cómo dejar de compartir un almacén de confianza
- Facturación y medición

## Requisitos previos para compartir un almacén de confianza

- Debe crear un recurso compartido utilizando AWS Resource Access Manager. Para obtener más información, consulte Crear un recurso compartido en la Guía del usuario de AWS RAM .
- Para compartir un almacén de confianza, debe ser propietario de él en su Cuenta de AWS. No puede compartir un almacén de confianza que se haya compartido con usted.
- Para compartir un almacén de confianza con su organización o con una unidad organizativa en AWS Organizations, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

## Permisos para almacenes de confianza compartidos

Propietarios de almacenes de confianza

- Los propietarios de almacenes de confianza pueden crear un almacén de confianza.
- Los propietarios de almacenes de confianza pueden usar un almacén de confianza con equilibradores de carga en la misma cuenta.
- Los propietarios de tiendas fiduciarias pueden compartir una tienda fiduciaria con otras AWS cuentas o AWS Organizations.
- Los propietarios de tiendas fiduciarias pueden dejar de compartir una tienda fiduciaria desde cualquier AWS cuenta o AWS Organizations.
- Los propietarios de almacenes de confianza no pueden impedir que los equilibradores de carga usen un almacén de confianza en la misma cuenta.
- Los propietarios de los almacenes de confianza pueden enumerar todos los Equilibradores de carga de aplicación mediante un almacén de confianza compartido.
- Los propietarios de almacenes de confianza pueden eliminar un almacén de confianza si no hay asociaciones actuales.
- Los propietarios de almacenes de confianza pueden eliminar las asociaciones con un almacén de confianza compartido.

- Los propietarios de tiendas de confianza reciben CloudTrail los registros cuando se utiliza una tienda de confianza compartida.

Consumidores de los almacenes de confianza

- Los consumidores de los almacenes de confianza pueden ver los almacenes de confianza compartidos.
- Los consumidores de un almacén de confianza pueden crear o modificar oyentes mediante un almacén de confianza en la misma cuenta.
- Los consumidores de un almacén de confianza pueden crear o modificar oyentes mediante un almacén de confianza compartido.
- Los consumidores de un almacén de confianza no pueden crear un oyente mediante un almacén de confianza que ya no sea de uso compartido.
- Los consumidores de los almacenes de confianza no pueden modificar un almacén de confianza compartido.
- Los consumidores de un almacén de confianza pueden ver el ARN de un almacén de confianza compartido cuando están asociados a un oyente.
- Los consumidores de un almacén de confianza reciben los CloudTrail registros al crear o modificar un oyente mediante un almacén de confianza compartido.

Permisos administrados

Al compartir un almacén de confianza, el recurso compartido utiliza permisos administrados para controlar qué acciones permite el consumidor del almacén de confianza. Puede utilizar los permisos administrados predeterminados `AWSRAMPermissionElasticLoadBalancingTrustStore`, que incluyen todos los permisos disponibles, o crear sus propios permisos administrados por el cliente. Los permisos `DescribeTrustStores`, `DescribeTrustStoreRevocations` y `DescribeTrustStoreAssociations` están siempre habilitados y no se pueden eliminar.

Los recursos compartidos del almacén de confianza admiten los siguientes permisos:

balanceo de carga elástico: CreateListener

Puede adjuntar un almacén de confianza compartido a un nuevo oyente.

equilibrio de carga elástico: ModifyListener

Puede adjuntar un almacén de confianza compartido a un oyente existente.

equilibrio de carga elástico: GetTrustStoreCaCertificatesBundle

Puede descargar el paquete de certificados de CA asociado al almacén de confianza compartido.

equilibrio de carga elástico: GetTrustStoreRevocationContent

Puede descargar el archivo de revocación asociado al almacén de confianza compartido.

elasticloadbalancing: (predeterminado) DescribeTrustStores

Puede enumerar todos los almacenes de confianza que pertenecen a la cuenta y que están compartidos con ella.

elasticloadbalancing: (predeterminado) DescribeTrustStoreRevocations

Puede enumerar todo el contenido de revocación del ARN del almacén de confianza en cuestión.

elasticloadbalancing: (predeterminado) DescribeTrustStoreAssociations

Puede enumerar todos los recursos de la cuenta de consumidor del almacén de confianza que están asociados al almacén de confianza compartido.

## Cómo compartir un almacén de confianza

Para compartir un almacén de confianza, debe añadirlo al recurso compartido. Un uso compartido de recursos es un recurso de AWS RAM que le permite compartir los recursos a través de Cuentas de AWS. Un recurso de uso compartido define los recursos a compartir, los consumidores con quienes se comparten y las acciones principales que pueden desempeñar. Cuando compartes un almacén de confianza mediante la EC2 consola de Amazon, lo añades a un recurso compartido existente. Para agregar el almacén de confianza a un nuevo recurso compartido, debe crear el recurso compartido mediante la consola de AWS RAM.

Cuando compartes un almacén de confianza de tu propiedad con otros Cuentas de AWS, permites que esas cuentas asocien sus dispositivos de escucha de Application Load Balancer a los almacenes de confianza de tu cuenta.

Si forma parte de una organización AWS Organizations y está habilitado el uso compartido dentro de su organización, los consumidores de su organización tienen acceso automático al almacén de confianza compartido. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso al almacén de confianza compartido después de aceptar la invitación.

Puedes compartir un almacén de confianza de tu propiedad mediante la EC2 consola de Amazon, la AWS RAM consola o la AWS CLI.

Para compartir un almacén de confianza de tu propiedad mediante la EC2 consola de Amazon

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrador de carga, elija Almacenes de confianza.
3. Seleccione el almacén de confianza para ver su página de detalles.
4. En la pestaña Compartir, elija Compartir almacén de confianza.
5. En la página Compartir almacén de confianza, en Recursos compartidos, seleccione con qué recursos compartidos quiere compartir su almacén de confianza.
6. (Opcional) Si necesita crear un nuevo recurso compartido, seleccione el enlace Crear un recurso compartido en la consola de RAM.
7. Seleccione Compartir almacén de confianza.

Para compartir un almacén de confianza de tu propiedad mediante la AWS RAM consola

Consulte Crear un recurso compartido en la Guía del usuario de AWS RAM .

Para compartir un almacén de confianza que sea de tu propiedad mediante AWS CLI

Utilice el comando create-resource-share.

## Cómo dejar de compartir un almacén de confianza

Para dejar de compartir un almacén de confianza de su propiedad, debe quitarlo del recurso compartido. Las asociaciones existentes persisten después de que deje de compartir su almacén de confianza; sin embargo, no se permite realizar nuevas asociaciones a un almacén de confianza que haya compartido previamente. Cuando el propietario del almacén de confianza o el consumidor de este eliminan una asociación, se elimina de ambas cuentas. Si el propietario de un almacén de confianza quiere dejar un recurso compartido, debe solicitar al propietario que elimine la cuenta.

> ⚠ Eliminación de una asociación
>
> Los propietarios de almacenes de confianza pueden eliminar forzosamente las asociaciones de almacenes de confianza existentes mediante el DeleteTrustStoreAssociationcomando. Cuando se elimina una asociación, cualquier oyente del equilibrador de carga que utilice el

almacén de confianza ya no podrá verificar los certificados de los clientes y no pasará los protocolos de enlace TLS.

Puedes dejar de compartir una tienda de confianza mediante la EC2 consola de Amazon, la AWS RAM consola o la AWS CLI.

Para dejar de compartir una tienda de confianza de tu propiedad mediante la EC2 consola de Amazon

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrador de carga, elija Almacenes de confianza.
3. Seleccione el almacén de confianza para ver su página de detalles.
4. En la pestaña Compartir, en Uso compartido de recursos, seleccione los recursos compartidos que quiere dejar de compartir.
5. Elija Eliminar.

Para dejar de compartir un almacén de confianza de tu propiedad mediante la AWS RAM consola

Consulte Actualizar un recurso compartido en la Guía del usuario de AWS RAM .

Para dejar de compartir un almacén de confianza de su propiedad mediante el AWS CLI

Utilice el comando disassociate-resource-share.

## Facturación y medición

Los almacenes de confianza compartidos tienen la misma tarifa estándar de almacén de confianza, que se factura por hora y por cada almacén de confianza asociado con un Equilibrador de carga de aplicación.

Para obtener más información, incluida la tarifa específica por región, consulte los precios de Elastic Load Balancing

# Autenticación de usuarios mediante un Equilibrador de carga de aplicación

Puede configurar un Equilibrador de carga de aplicación para autenticar de forma segura a los usuarios cuando obtienen acceso a sus aplicaciones. Esto le permite liberar a su equilibrador 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 identidades (IdP) compatible con OpenID Connect (OIDC).
- Autentique a los usuarios a través de las redes sociales IdPs, como Amazon, Facebook o Google, a través de los grupos de usuarios compatibles con Amazon Cognito.
- Autentique a los usuarios mediante identidades corporativas, mediante SAML, OpenID Connect (OIDC) o OAuth mediante los grupos de usuarios compatibles con Amazon Cognito.

## Preparativos para usar un IdP compatible con OIDC

Haga lo siguiente si utiliza un IdP compatible con OIDC con su Equilibrador de carga de aplicación:

- Cree una nueva aplicación OIDC en su IdP. El DNS del IdP debe poder resolverse públicamente.
- 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.
- Los certificados de los puntos de conexión del IdP deben ser emitidos por una autoridad de certificación pública de confianza.
- Las entradas de DNS de los puntos de conexión deben poder resolverse públicamente, incluso si se resuelven en direcciones IP privadas.
- Permite una de las siguientes redirecciones URLs en tu aplicación de IdP, sea cual sea la que usen tus usuarios, donde DNS es el nombre de dominio de tu balanceador de cargas y CNAME es el alias de DNS de tu aplicación:
  - https:///oauth2/idpresponse *DNS*
  - *CNAME*https://oauth2/idpresponse

# Preparación para usar Amazon Cognito

## Regiones disponibles

La integración de Amazon Cognito para los Equilibradores de carga de aplicación está disponible en las siguientes regiones:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)
- Canadá (centro)
- Oeste de Canadá (Calgary)
- Europa (Estocolmo)
- Europa (Milán)
- Europa (Fráncfort)
- Europa (Zúrich)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- Europa (España)
- América del Sur (São Paulo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Tokio)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)

- Medio Oriente (EAU)
- Medio Oriente (Baréin)
- África (Ciudad del Cabo)
- Israel (Tel Aviv)

Haga lo siguiente si utiliza grupos de usuarios de Amazon Cognito con su Equilibrador de carga de aplicación:

- 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 del grupo de usuarios. Debes configurar el cliente para que genere un secreto de cliente, utilice el flujo de concesión de código y admita los mismos OAuth ámbitos que utiliza el balanceador de cargas. 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 Configurar un dominio de 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 Inicio de sesión en grupos de usuarios con un proveedor de identidad externo en la Guía para desarrolladores de Amazon Cognito.
- Permita la siguiente redirección URLs en el campo URL de devolución de llamada de Amazon Cognito, donde DNS es el nombre de dominio del balanceador de carga y CNAME es el alias de DNS de su aplicación (si está utilizando uno):
  - https:///oauth2/idpresponse *DNS*
  - *CNAME*https://oauth2/idpresponse
- Permita 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:
  - *domain-prefix*https://.auth. *region*.amazoncognito. com/saml2/idpresponse
  - *user-pool-domain*https://saml2/idpreresponse

La URL de devolución de llamada de la configuración del cliente de la aplicación debe estar compuesta exclusivamente por letras minúsculas.

Para permitir que un usuario pueda configurar un equilibrador 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`.

## Prepárate para usar Amazon CloudFront

Active los siguientes ajustes si utiliza una CloudFront distribución delante de su Application Load Balancer:

- Reenviar los encabezados de las solicitudes (todos): garantiza que CloudFront no se almacenen en caché las respuestas de las solicitudes autenticadas. Esto evita que se sirvan desde la caché después de que venza la sesión de autenticación. Como alternativa, para reducir este riesgo mientras el almacenamiento en caché está activado, los propietarios de una CloudFront distribución pueden configurar el valor time-to-live (TTL) para que caduque antes de que caduque la cookie de autenticación.
- Reenvío y almacenamiento en caché de cadenas de consulta (todos): garantiza que el equilibrador de carga tenga acceso a los parámetros de la cadena de consulta necesarios para autenticar al usuario con el IdP.
- Reenvío de cookies (todas): garantiza que se CloudFront reenvíen todas las cookies de autenticación al balanceador de cargas.
- Al configurar la autenticación OpenID Connect (OIDC) junto con Amazon CloudFront, asegúrese de que el puerto HTTPS 443 se utilice de forma coherente en toda la ruta de conexión. De lo contrario, se pueden producir errores de autenticación porque la redirección OIDC del cliente URLs no coincide con el número de puerto del URI generado originalmente.

## Configuración de la autenticación de usuarios

La autenticación de usuario se configura creando una acción de autenticación para una o varias reglas de oyente. Los tipos de acción `authenticate-cognito` y `authenticate-oidc` solo se admiten con oyentes HTTPS. Para obtener descripciones de los campos correspondientes, consulte AuthenticateCognitoActionConfigy AuthenticateOidcActionConfigen la versión 2015-12-01 de referencia de la API de Elastic Load Balancing.

El equilibrador de carga envía una cookie de sesión al cliente para mantener el estado de autenticación. Esta cookie siempre contiene el atributo `secure`, porque la autenticación del usuario

requiere un oyente HTTPS. Esta cookie contiene el atributo `SameSite=None` con solicitudes CORS (intercambio de recursos de varios orígenes).

En el caso de un equilibrador de carga compatible con varias aplicaciones que requieren una autenticación de cliente independiente, cada regla de oyente con una acción de autenticación debe tener un nombre de cookie único. Esto garantiza que los clientes estén siempre autenticados con el IdP antes de ser enrutados al grupo de destino especificado en la regla.

Los equilibradores de carga de aplicaciones no admiten valores de cookies codificados como URL.

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 Tiempo de espera de la sesión.

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

- Aplicaciones que requieren que el usuario inicie sesión mediante una identidad social o corporativa: se admite mediante la opción predeterminada `authenticate`. Si el usuario no ha iniciado sesión, el equilibrador de carga redirige la solicitud al punto de conexión 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 equilibrador de carga proporciona las notificaciones de usuario y la aplicación puede ofrecer una vista personalizada. Si el usuario no ha iniciado sesión, el equilibrador de carga reenvía la solicitud sin las notificaciones de usuario y la aplicación puede proporcionar la vista general.
- Aplicaciones de una sola página JavaScript que se cargan cada pocos segundos: si utilizas **deny** esta opción, el balanceador de cargas devuelve un error HTTP 401 no autorizado a las llamadas AJAX que no contienen información de autenticación. Sin embargo, si la información de autenticación del usuario ha caducado, redirige al cliente al punto de conexión de autorización del IdP.

El equilibrador de carga debe poder comunicarse con el punto de conexión de token de IdP (`TokenEndpoint`) y el punto de conexión de información de usuario de IdP (`UserInfoEndpoint`). Los balanceadores de carga de aplicaciones solo son compatibles IPv4 cuando se comunican con estos puntos finales. Si su IdP usa direcciones públicas, asegúrese de que los grupos de seguridad del balanceador de cargas y la red de la ACLs VPC permitan el acceso a los puntos finales. Cuando

se utiliza un equilibrador de carga interno o el tipo de dirección IP `dualstack-without-public-ipv4`, una puerta de enlace NAT puede permitir que el equilibrador de carga se comunique con los puntos de conexión. Para obtener más información, consulte Información básica de puertas de enlace NAT en la Guía del usuario de Amazon VPC.

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
```

A continuación se muestra un ejemplo del archivo `actions.json` que especifica una acción `authenticate-oidc` y una acción `forward`. `AuthenticationRequestExtraParams` le permite pasar parámetros adicionales a un IdP durante la autenticación. Siga la documentación proporcionada por su proveedor de identidades para determinar los campos que son compatibles

```
[{
    "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
}]
```

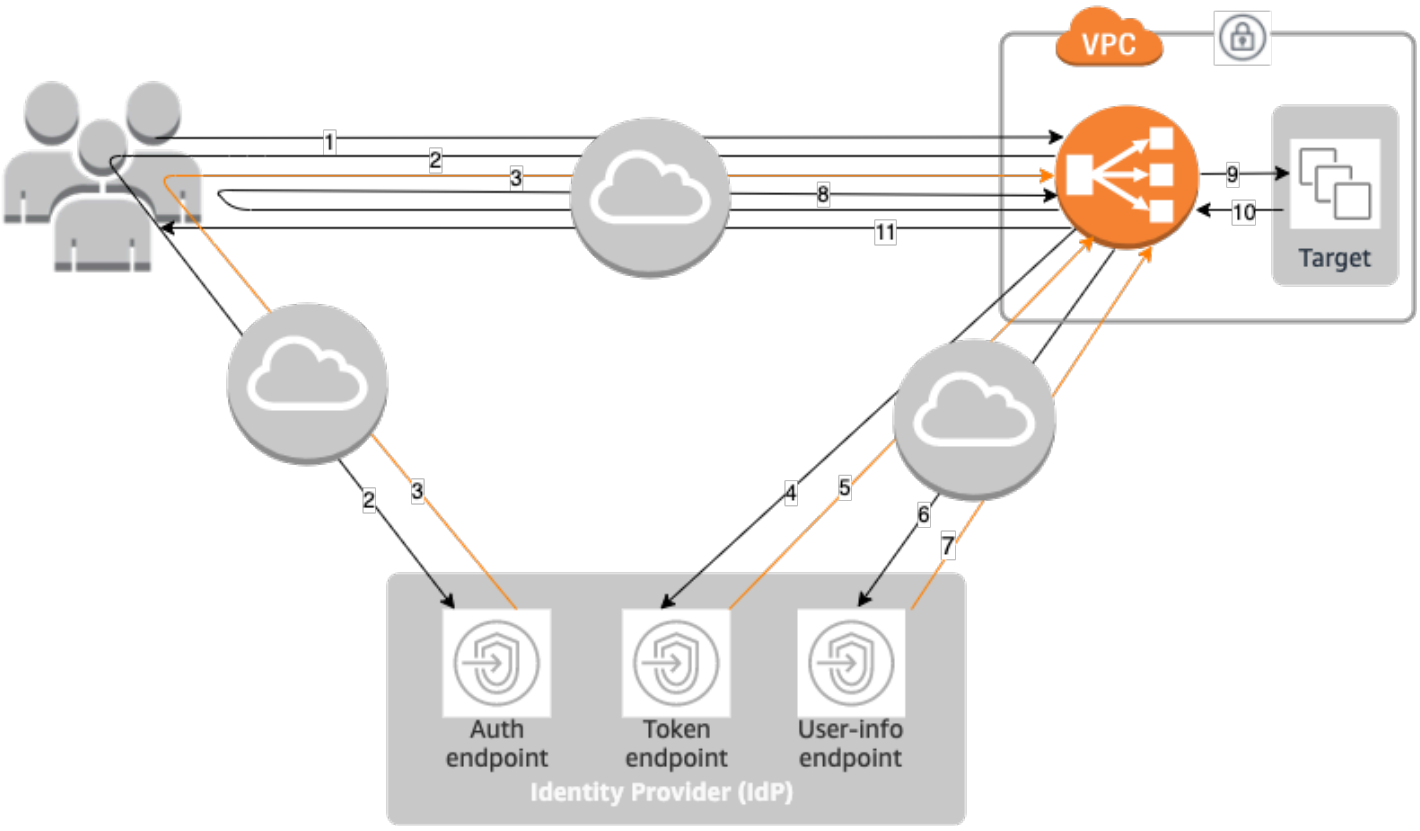
El siguiente es un ejemplo del archivo `actions.json` que especifica las acciones `authenticate-cognito` y `forward`.

```
[{
    "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 oyente.

## Flujo de autenticación

El siguiente diagrama de red es una representación visual de cómo un Equilibrador de carga de aplicación utiliza OIDC para autenticar a los usuarios.




Los elementos numerados que siguen, destacan y explican los elementos que se muestran en el diagrama de red anterior.

1. El usuario envía una solicitud HTTPS a un sitio web alojado detrás de un Equilibrador de carga de aplicación. Cuando se cumplen las condiciones de una regla con una acción de autenticación, el equilibrador de carga comprueba si hay una cookie de sesión de autenticación en los encabezados de solicitudes.
2. Si la cookie no está presente, el equilibrador de carga redirige al usuario al punto de conexión de autorización de IdP para que el IdP pueda autenticarlo.
3. Después de autenticar al usuario, el IdP lo redirige al equilibrador de carga con un código de concesión de autorización.
4. El equilibrador de carga presenta el código de concesión de autorización al punto de conexión del token de IdP.
5. Al recibir un código de concesión de autorización válido, el IdP proporciona el token de identificación y el token de acceso al Equilibrador de carga de aplicación.
6. A continuación, el Equilibrador de carga de aplicación envía el token de acceso al punto de conexión de información del usuario.

7. El punto de conexión de información del usuario intercambia el token de acceso por las solicitudes de los usuarios.
8. El Equilibrador de carga de aplicación redirige al usuario con la cookie de sesión de autenticación de `AWSELB` al URI original. Debido a que la mayoría de los navegadores limitan una cookie a 4 KB de tamaño, el equilibrador 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 equilibrador de carga devuelve un error HTTP 500 al cliente y aumenta la métrica `ELBAuthUserClaimsSizeExceeded`.
9. El Equilibrador de carga de aplicación valida la cookie y reenvía la información del usuario a los destinos del conjunto de encabezados HTTP de `X-AMZN-OIDC-*`. Para obtener más información, consulte Codificación de las notificaciones de usuario y verificación de firmas.
10. El destino envía una respuesta al Equilibrador de carga de aplicación.
11. El Equilibrador de carga de aplicación envía la respuesta final al usuario.

Cada nueva solicitud atraviesa los pasos 1 a 11, mientras que las solicitudes posteriores atraviesan los pasos 9 a 11. Es decir, todas las solicitudes subsiguientes comienzan en el paso 9 siempre que la cookie no haya caducado.

La cookie de `AWSALBAuthNonce` se agrega al encabezado de la solicitud después de que el usuario se autentique en el IdP. Esto no cambia la forma en que Equilibrador de carga de aplicación procesa las solicitudes de redireccionamiento del IdP.

Si el IdP proporciona un token de actualización válido en el token de ID, el equilibrador 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 equilibrador de carga redirige al usuario al punto de conexión de autorización de IdP. De este modo, el equilibrador de carga puede dejar de funcionar después de que el usuario cierre la sesión. Para obtener más información, consulte Tiempo de espera de la sesión.

> **Note**
>
> La caducidad de la cookie es diferente de la caducidad de la sesión de autenticación. La caducidad de la cookie es un atributo de la cookie, que se establece en 7 días. La duración real de la sesión de autenticación viene determinada por el tiempo de espera de la sesión configurado en el Equilibrador de carga de aplicación para la característica de autenticación.

El tiempo de espera de la sesión se incluye en el valor de la cookie de autenticación, que también está cifrado.

## Codificación de las notificaciones de usuario y verificación de firmas

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

El equilibrador de carga añade los siguientes encabezados HTTP:

`x-amzn-oidc-accesstoken`

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

`x-amzn-oidc-identity`

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

Nota: La subreclamación es la mejor forma de identificar a un usuario determinado.

`x-amzn-oidc-data`

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

Los tokens de acceso y las reclamaciones de los usuarios son diferentes de los tokens de identificación. Los tokens de acceso y las reclamaciones de usuario solo permiten el acceso a los recursos del servidor, mientras que los tokens contienen información adicional para autenticar a un usuario. El Equilibrador de carga de aplicación crea un token de acceso nuevo cuando autentica al usuario y solo pasa los tokens de acceso y las reclamaciones al backend, pero no pasa la información del token de identificación.

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. Un Application Load Balancer utiliza ES256 (ECDSA con P-256 y SHA256) para generar la firma JWT.

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 conexión de información de usuario de IdP.

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

Si quiere que el equilibrador de carga cifre las reclamaciones de los usuarios, debe configurar su grupo de destino para que use HTTPS. Además, como práctica recomendada de seguridad, le recomendamos que restrinja sus destinos para que solo reciban tráfico de su Equilibrador de carga de aplicación. Para ello, configure el grupo de seguridad del destino para que haga referencia al ID del grupo de seguridad del equilibrador de carga.

Para garantizar la seguridad, debe verificar la firma antes de realizar cualquier autorización basada en las notificaciones y validar que el campo `signer` del encabezado JWT contenga el ARN esperado del Equilibrador de carga de aplicación.

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 conexión regional. El punto de conexión de cada región de AWS es el siguiente:

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

Para ello AWS GovCloud (US), los puntos finales son los siguientes:

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

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

AWS proporciona una biblioteca que puede usar para verificar si está JWTs firmada por Amazon Cognito, Application Load Balancers y otros dispositivos compatibles con OIDC. IDPs Para obtener más información, consulte JWT Verify.AWS

# Tiempo de espera

## Tiempo de espera de 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 más corto que la fecha de vencimiento del token de acceso, el equilibrador de carga respeta el tiempo de espera de la sesión. Si el usuario tiene una sesión activa con el IdP, es posible que no se le pida que inicie sesión de nuevo. De lo contrario, se redirige al usuario para que inicie sesión.
  - Si el tiempo de espera de la sesión del IdP es superior al tiempo de espera de la sesión de Equilibrador de carga de aplicación, el usuario no tiene que proporcionar credenciales para volver a iniciar sesión. En su lugar, el IdP se redirige de nuevo al Equilibrador de carga de aplicación con un nuevo código de concesión de autorización. Los códigos de autorización son de un solo uso, incluso si no hay que volver a iniciar sesión.
  - Si el tiempo de espera de la sesión del IdP es igual o inferior al tiempo de espera de la sesión de Equilibrador de carga de aplicación, se le pide al usuario que proporcione las credenciales para volver a iniciar sesión. Una vez que el usuario inicia sesión, el IdP se redirige de nuevo al Equilibrador de carga de aplicación con un nuevo código de concesión de autorización, y el resto del flujo de autenticación continúa hasta que la solicitud llegue al backend.
- 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 equilibrador 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. Luego, hace que el usuario vuelva a iniciar sesión.
- 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 equilibrador de carga actualiza la sesión de usuario cada vez que vence el token de acceso. El equilibrador 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.

### Tiempo de espera de inicio de sesión de cliente

El cliente debe iniciar y completar el proceso de autenticación en 15 minutos. Si un cliente no completa la autenticación dentro del límite de 15 minutos, recibe un error HTTP 401 del equilibrador de carga. Este tiempo de espera no se puede cambiar ni eliminar.

Por ejemplo, si un usuario carga la página de inicio de sesión a través del Equilibrador de carga de aplicación, debe completar el proceso de inicio de sesión en 15 minutos. Si el usuario espera e intenta iniciar sesión una vez transcurrido el tiempo de espera de 15 minutos, el equilibrador de carga devuelve un error HTTP 401. El usuario tendrá que actualizar la página e intentar iniciar sesión de nuevo.

## Cierre de sesión de autenticación

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 conexión 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 al balanceador de cargas una cookie de sesión que tiene un token de acceso caducado con un token de actualización que no es NULL, el balanceador de cargas contacta con el IdP para determinar si el usuario sigue conectado.

Las páginas de inicio de sesión del cliente no están autenticadas. Esto significa que no pueden estar detrás de una regla de Application Load Balancer que requiera autenticación.

- Cuando se envía una solicitud al destino, la aplicación debe establecer la caducidad en -1 para todas las cookies de autenticación. Los equilibradores de carga de aplicaciones admiten cookies con un tamaño de hasta 16 KB y, por lo tanto, pueden crear hasta 4 particiones para enviarlas al cliente.
  - Si el IdP tiene un punto de conexión de cierre de sesión, debería emitir una redirección al punto de conexión de cierre de sesión del IdP, por ejemplo, el punto de conexión LOGOUT documentado en la Guía para desarrolladores de Amazon Cognito.
  - Si el IdP no tiene un punto de conexión de cierre de sesión, la solicitud vuelve a la página de inicio de cierre de sesión del cliente y se reinicia el proceso de inicio de sesión.
- Si se supone que el IdP tiene un punto de conexión de cierre de sesión, el IdP debe caducar los tokens de acceso y actualizarlos, y redirigir al usuario de nuevo a la página de inicio de sesión del cliente.
- Las solicitudes posteriores siguen el flujo de autenticación original.

# Etiquetas para las reglas y los oyentes del Equilibrador de carga de aplicación

Las etiquetas ayudan a clasificar a los oyentes y las reglas de diversas maneras. Por ejemplo, puede etiquetar un recurso por objetivo, propietario o entorno.

Puede agregar varias etiquetas a cada oyente y regla. Las claves de las etiquetas deben ser únicas para cada oyente y regla. Si agrega una etiqueta con una clave que ya está asociada al oyente y la regla, se actualiza el valor de esa etiqueta.

Cuando ya no necesite una etiqueta, puede eliminarla.

Restricciones

- Número máximo 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 iniciales ni finales.
- No utilice el `aws:` prefijo en los nombres o valores de las etiquetas, ya que está reservado para AWS su uso. Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar ni eliminar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.

## Actualizar las etiquetas de oyente

Para actualizar las etiquetas de un oyente desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga que contiene el oyente que desea actualizar para abrir su página de detalles.
4. En la pestaña Oyentes y reglas, realice alguna de las siguientes acciones:

    a. Seleccione el texto de la columna Protocolp:Puerto para abrir la página de detalles del oyente.

En la pestaña Etiquetas, elija Administrar etiquetas.

b. Seleccione el oyente en el que desea actualizar las etiquetas.

   Seleccione Administrar el oyente y, a continuación, Administrar etiquetas.

c. Seleccione el texto de la columna Etiquetas para abrir la página de detalles del oyente, en la pestaña Etiquetas.

   Elija Administrar etiquetas.

5. En la página Administrar etiquetas, puede hacer lo siguiente:

   a. Para actualizar una etiqueta, ingrese valores nuevos para Clave y Valor.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta nueva y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.

6. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de un oyente mediante el AWS CLI

Utilice los comandos add-tags y remove-tags.

## Actualizar las etiquetas de reglas

Para actualizar las etiquetas de una regla desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga que contiene la regla que desea actualizar para abrir su página de detalles.
4. En la pestaña Oyentes y reglas, elija el texto de la columna Protocolo:Puerto del oyente que contiene la regla que desea actualizar, para abrir la página de detalles del oyente.
5. En la página de detalles del oyente, realice una de las siguientes operaciones:

   a. Seleccione el texto de la columna Etiqueta de nombre para abrir la página de detalles de la regla.

      En la página Detalles de la regla, elija Editar.

   b. Seleccione el texto de la columna Etiquetas para la regla que desee actualizar.

En la ventana emergente de resumen de etiquetas, seleccione Administrar etiquetas.

6. En la página Administrar etiquetas, puede hacer lo siguiente:
   a. Para actualizar una etiqueta, ingrese valores nuevos para Clave y Valor.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta nueva y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.
7. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de una regla, usa el AWS CLI

Utilice los comandos add-tags y remove-tags.

# Eliminar un oyente de Equilibrador de carga de aplicación

Puede eliminar un oyente en cualquier momento. Cuando se elimina un equilibrador de carga, se eliminan todos sus oyentes.

Cómo eliminar un oyente a través de la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, seleccione la casilla de verificación del oyente y elija Administrar oyente, Eliminar oyente.
5. Cuando se le pida confirmación, ingrese **`confirm`** y elija Eliminar.

Para eliminar un oyente mediante el AWS CLI

Utilice el comando delete-listener.

# Modificación del encabezado HTTP de su Application Load Balancer

Los balanceadores de carga de aplicaciones admiten la modificación del encabezado HTTP, tanto para los encabezados de solicitud como de respuesta. Sin tener que actualizar el código de la

aplicación, la modificación del encabezado le permite tener un mayor control sobre el tráfico y la seguridad de la aplicación.

Para habilitar la modificación del encabezado, consulte[Habilite la modificación del encabezado](#).

## Cambie el nombre de mTLS/TLS los encabezados

La capacidad de cambiar el nombre de los encabezados le permite configurar los nombres de los encabezados mTLS y TLS que Application Load Balancer genera y agrega a las solicitudes.

Esta capacidad de modificar los encabezados HTTP permite a Application Load Balancer admitir fácilmente aplicaciones que utilizan encabezados de solicitud y respuesta con un formato específico.

| Encabezado | Descripción |
|---|---|
| X-Amzn-Mtls-Clientcert-Serial-Number | Garantiza que el destinatario pueda identificar y verificar el certificado específico presentado por el cliente durante el protocolo de enlace TLS. |
| X-Amzn-Mtls-Clientcert-Issuer | Ayuda al objetivo a validar y autenticar el certificado del cliente al identificar a la autoridad de certificación que emitió el certifica do. |
| X-Amzn-Mtls-Clientcert-Subject | Proporciona al destinatario información detallada sobre la entidad a la que se emitió el certificado de cliente, lo que ayuda a identific ar, autenticar, autorizar y registrar durante la autenticación mTLS. |
| X-Amzn-Mtls-Clientcert-Validity | Permite al destinatario comprobar que el certificado de cliente que se está utilizando se encuentra dentro del período de validez definido, lo que garantiza que el certificado no haya caducado ni se haya utilizado de forma prematura. |
| X-Amzn-Mtls-Clientcert-Leaf | Proporciona el certificado de cliente utilizado en el protocolo de enlace mTLS, lo que permite al |

| Encabezado | Descripción |
| --- | --- |
| | servidor autenticar al cliente y validar la cadena de certificados. Esto garantiza que la conexión sea segura y esté autorizada. |
| X-Amzn-Mtls-Clientcert | Incluye el certificado de cliente completo. Permite al destinatario verificar la autenticidad del certificado, validar la cadena de certifica dos y autenticar al cliente durante el proceso de protocolo de enlace mTLS. |
| X-Amzn-TLS-Version | Indica la versión del protocolo TLS utilizada para una conexión. Facilita la determinación del nivel de seguridad de la comunicación, la resolución de problemas de conexión y la garantía de la conformidad. |
| X-Amzn-TLS-Cipher-Suite | Indica la combinación de algoritmos criptográ ficos que se utilizan para proteger una conexión en TLS. Esto permite al servidor evaluar la seguridad de la conexión, lo que ayuda a solucionar problemas de compatibi lidad y garantiza el cumplimiento de las políticas de seguridad. |

## Agregue encabezados de respuesta

Con los encabezados de inserción, puede configurar su Application Load Balancer para añadir encabezados relacionados con la seguridad a las respuestas. Con estos atributos, puede insertar encabezados que incluyan HSTS, CORS y CSP.

De forma predeterminada, estos encabezados están vacíos. Cuando esto ocurre, Application Load Balancer no modifica este encabezado de respuesta.

Al habilitar un encabezado de respuesta, Application Load Balancer agrega el encabezado con el valor configurado a todas las respuestas. Si la respuesta del destino incluye el encabezado de respuesta HTTP, el balanceador de cargas actualiza el valor del encabezado para que sea el valor

configurado. De lo contrario, el balanceador de cargas agrega el encabezado de respuesta HTTP a la respuesta con el valor configurado.

| Encabezado | Descripción |
| --- | --- |
| Strict-Transport-Security | Hace que el navegador solo establezca conexiones HTTPS durante un período específico, lo que ayuda a protegerlo contra man-in-the-middle los ataques, las degradaciones de protocolo y los errores de los usuarios, y garantiza que todas las comunicaciones entre el cliente y el objetivo estén cifradas. |
| Access-Control-Allow-Origin | Controla si se puede acceder a los recursos de un objetivo desde distintos orígenes. Esto permite interacciones seguras entre orígenes y, al mismo tiempo, evita el acceso no autorizado. |
| Access-Control-Allow-Methods | Especifica los métodos HTTP que se permiten al realizar solicitudes de origen cruzado al destino. Proporciona control sobre qué acciones se pueden realizar desde diferentes orígenes. |
| Access-Control-Allow-Headers | Especifica qué encabezados personalizados o no simples se pueden incluir en una solicitud de origen cruzado. Este encabezado permite a los destinatarios controlar qué encabezados pueden enviar clientes de diferentes orígenes. |
| Access-Control-Allow-Credentials | Especifica si el cliente debe incluir credenciales como cookies, autenticación HTTP o certificados de cliente en las solicitudes de origen cruzado. |
| Access-Control-Expose-Headers | Permite al destinatario especificar a qué encabezados de respuesta adicionales puede |

| Encabezado | Descripción |
| --- | --- |
| | acceder el cliente en las solicitudes de origen cruzado. |
| Access-Control-Max-Age | Define durante cuánto tiempo el navegador puede almacenar en caché el resultado de una solicitud de verificación previa, lo que reduce la necesidad de realizar comprobac iones previas repetidas. Esto ayuda a optimizar el rendimiento al reducir el número de solicitud es de opciones necesarias para determinadas solicitudes de origen cruzado. |
| Content-Security-Policy | Función de seguridad que evita los ataques de inyección de código, como el XSS, al controlar qué recursos, como scripts, estilos, imágenes, etc., puede cargar y ejecutar un sitio web. |
| X-Content-Type-Options | Con la directiva antirastreo, mejora la seguridad web al evitar que los navegadores adivinen el tipo MIME de un recurso. Garantiza que los navegadores solo interpreten el contenido de acuerdo con el tipo de contenido declarado |
| X-Frame-Options | Mecanismo de seguridad de encabezados que ayuda a prevenir los ataques de secuestro de clics al controlar si una página web se puede incrustar en marcos. Valores como DENY y SAMEORIGIN pueden garantizar que el contenido no se incruste en sitios web malintencionados o que no sean de confianza. |

## Deshabilita los encabezados

Con los encabezados de desactivación, puede configurar su Application Load Balancer para deshabilitar `server:awselb/2.0` el encabezado de las respuestas. Esto reduce la exposición de la información específica del servidor y, al mismo tiempo, añade una capa adicional de protección a la aplicación.

El nombre del atributo es`routing.http.response.server.enabled`. Los valores disponibles son `true` o`false`. El valor predeterminado es `true`.

## Limitaciones

- Los valores del encabezado pueden contener los siguientes caracteres
  - Caracteres alfanuméricos: `a-z`, `A-Z`, y `0-9`
  - Caracteres especiales: `_ :;.,\/'?!(){}[]@<>=-+*#&`|~^%`
- El valor del atributo no puede superar los 1000 bytes de tamaño.
- Elastic Load Balancing realiza validaciones de entrada básicas para comprobar que el valor del encabezado es válido. Sin embargo, la validación no puede confirmar si el valor es compatible con un encabezado específico.
- Si se establece un valor vacío para cualquier atributo, el Application Load Balancer volverá al comportamiento predeterminado.

## Habilite la modificación del encabezado HTTP para su Application Load Balancer

La modificación del encabezado está desactivada de forma predeterminada y debe estar habilitada en todos los oyentes.

Para habilitar la modificación del encabezado mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione Application Load Balancer.
4. En la pestaña Listeners and rules, seleccione el protocolo y el puerto para abrir la página de detalles del listener.
5. En la pestaña Atributos, seleccione Editar.

Los atributos de los oyentes se organizan en grupos. Escogerá qué funciones desea habilitar.

6. [Oyentes de HTTPS] Nombres de cabecera modificables mTLS/TLS

   a. Amplíe los nombres de los encabezados modificables mTLS/TLS .

   b. Habilite los encabezados de las solicitudes para modificarlos y proporcione nombres para ellos. Para obtener más información, consulte the section called “Cambie el nombre de mTLS/TLS los encabezados”.

7. Agregue encabezados de respuesta

   a. Amplíe Agregar encabezados de respuesta.

   b. Habilite los encabezados de respuesta para agregarles y proporcionarles valores. Para obtener más información, consulte the section called “Agregue encabezados de respuesta”.

8. Cabecera de respuesta del servidor ALB

   - Habilite o deshabilite el encabezado del servidor.

9. Seleccione Save changes (Guardar cambios).

Para habilitar la modificación del encabezado mediante el AWS CLI

Utilice el modify-listener-attributescomando con los siguientes atributos:

`routing.http.request.x_amzn_mtls_clientcert_serial_number.header_name`

Modifique el nombre del encabezado de X-Amzn-Mtls-Clientcert-Serial-Number.

`routing.http.request.x_amzn_mtls_clientcert_issuer.header_name`

Modifique el nombre del encabezado de X-Amzn-Mtls-Clientcert-Issuer.

`routing.http.request.x_amzn_mtls_clientcert_subject.header_name`

Modifique el nombre del encabezado de X-Amzn-Mtls-Clientcert-Subject.

`routing.http.request.x_amzn_mtls_clientcert_validity.header_name`

Modifique el nombre del encabezado de X-Amzn-Mtls-Clientcert-Validity.

`routing.http.request.x_amzn_mtls_clientcert_leaf.header_name`

Modifique el nombre del encabezado de X-Amzn-Mtls-Clientcert-Leaf.

`routing.http.request.x_amzn_mtls_clientcert.header_name`

Modifique el nombre del encabezado de X-Amzn-Mtls-Clientcert.

`routing.http.request.x_amzn_tls_version.header_name`

Modifique el nombre del encabezado de X-Amzn-Tls-Version.

`routing.http.request.x_amzn_tls_cipher_suite.header_name`

Modifique el nombre del encabezado de X-Amzn-Tls-Cipher-Suite.

`routing.http.response.server.enabled`

Indica si se debe permitir o eliminar el encabezado del servidor de respuesta HTTP.

`routing.http.response.strict_transport_security.header_value`

Agregue el encabezado Strict-Transport-Security para informar a los navegadores de que solo se debe acceder al sitio mediante HTTPS y que cualquier intento futuro de acceder a él mediante HTTP se convertirá automáticamente a HTTPS.

`routing.http.response.access_control_allow_origin.header_value`

Añada el encabezado Access-Control-Allow-Origin para especificar qué orígenes pueden acceder al servidor.

`routing.http.response.access_control_allow_methods.header_value`

Agregue el encabezado Access-Control-Allow-Methods para especificar qué métodos HTTP están permitidos cuando se accede al servidor desde un origen diferente.

`routing.http.response.access_control_allow_headers.header_value`

Agregue el encabezado Access-Control-Allow-Headers para especificar qué encabezados están permitidos durante una solicitud de origen cruzado.

`routing.http.response.access_control_allow_credentials.header_value`

Agrega el encabezado Access-Control-Allow-Credentials para indicar si el navegador debe incluir credenciales, como cookies o de autenticación, en las solicitudes de origen cruzado.

`routing.http.response.access_control_expose_headers.header_value`

Agregue el encabezado Access-Control-Expose-Headers para indicar qué encabezados puede mostrar el navegador al cliente solicitante.

`routing.http.response.access_control_max_age.header_value`

Añada el encabezado Access-Control-Max-Age para especificar durante cuánto tiempo se pueden almacenar en caché los resultados de una solicitud de verificación previa, en segundos.

`routing.http.response.content_security_policy.header_value`

Añada el encabezado Content-Security-Policy para especificar las restricciones impuestas por el navegador y así minimizar el riesgo de determinados tipos de amenazas a la seguridad.

`routing.http.response.x_content_type_options.header_value`

Añada el encabezado X-Content-Type-Options para indicar si se deben seguir los tipos de MIME anunciados en los encabezados de Content-Type y no se deben cambiar.

`routing.http.response.x_frame_options.header_value`

Añada el encabezado X-Frame-Options para indicar si el navegador puede representar una página en un marco, iframe, incrustación u objeto.

# Grupos de destino para los equilibradores de carga de aplicaciones

Los grupos de destino dirigen las solicitudes a destinos individuales registrados, como EC2 instancias, mediante el protocolo y el número de puerto que especifique. 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 oyente del equilibrador de carga.

Cada grupo de destino se utiliza para direccionar solicitudes a uno o varios destinos registrados. Cuando se crea la regla de cada oyente, 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. Puede usar cada grupo de destino con un solo equilibrador de carga. Para obtener más información, consulte Componentes del Equilibrador de carga de aplicación.

Puede definir la configuración de comprobación de estado del equilibrador 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 oyente, el equilibrador 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 equilibrador de carga. El equilibrador de carga direcciona las solicitudes a los destinos registrados que se encuentran en buen estado.

Contenido

- Estado del grupo de destino
- Creación de un grupo de destino para el Equilibrador de carga de aplicación
- Actualización de la configuración de estado del grupo de destino del Equilibrador de carga de aplicación
- Comprobaciones de estado de los grupos de destinos del Equilibrador de carga de aplicación.
- Edición de los atributos del grupo de destino del Equilibrador de carga de aplicación
- Registro de destinos con el grupo de destino del Equilibrador de carga de aplicación
- Uso de funciones de Lambda como destino de un Equilibrador de carga de aplicación
- Etiquetas para el grupo de destino del Equilibrador de carga de aplicación
- Eliminación de un grupo de destino del Equilibrador de carga de aplicación

## Configuración de enrutamiento

De forma predeterminada, un equilibrador 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 dirigir el tráfico a un destino al registrarlo en el grupo de destino.

Los grupos de destino admiten los siguientes protocolos y puertos:

- Protocolos: HTTP, HTTPS
- Puertos: 1-65535

Cuando un grupo de destino se configura con el protocolo HTTPS o utiliza comprobaciones de estado de HTTPS, si algún oyente de HTTPS utiliza una política de seguridad TLS 1.3, la política de seguridad `ELBSecurityPolicy-TLS13-1-0-2021-06` se utilizará en las conexiones de destino. De lo contrario, se utiliza la política de seguridad `ELBSecurityPolicy-2016-08`. El equilibrador de carga establece conexiones TLS con los destinos mediante certificados que instala en los destinos. El equilibrador de carga no valida estos certificados. Por lo tanto, puede utilizar certificados autofirmados o certificados que hayan caducado. Como el balanceador de cargas y sus objetivos se encuentran en una nube privada virtual (VPC), el tráfico entre el balanceador de cargas y los destinos se autentica a nivel de paquete, por lo que no corre el riesgo man-in-the-middle de sufrir ataques o suplantación de identidad aunque los certificados de los destinos no sean válidos. El tráfico que salga no AWS tendrá las mismas protecciones, por lo que es posible que se necesiten medidas adicionales para proteger aún más el tráfico.

# 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 que crea 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 de 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)

> **Important**
>
> No puede especificar direcciones IP direccionables públicamente.

Todos los bloques CIDR compatibles le permiten registrar los siguientes destinos en un grupo de destino:

- Instancias en una VPC que está interconectada a la VPC del equilibrador de carga (misma región o región diferente).

- AWS recursos direccionables por dirección IP y puerto (por ejemplo, bases de datos).
- Recursos locales vinculados a una conexión a AWS través de una VPN AWS Direct Connect o a una Site-to-Site conexión VPN.

> **Note**
>
> En el caso de los equilibradores de carga de aplicaciones implementados en una zona local, los destinos `ip` deben estar en la misma zona local para recibir tráfico.
> Para obtener más información, consulte ¿Qué son las Zonas AWS Locales?

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 de Lambda. Cuando el equilibrador de carga recibe una solicitud para la función de Lambda, invoca la función de Lambda. Para obtener más información, consulte Uso de funciones de Lambda como destino de un Equilibrador de carga de aplicación.

Puede configurar Amazon Elastic Container Service (Amazon ECS) como destino de Equilibrador de carga de aplicación. Para obtener más información, consulte Use an Application Load Balancer para Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

## Tipo de dirección IP

Al crear un nuevo grupo de destino, puede seleccionar el tipo de dirección IP de su grupo de destino. Esto controla la versión de IP utilizada para comunicarse con los destinos y comprobar su estado.

Los grupos objetivo de los balanceadores de carga de aplicaciones admiten los siguientes tipos de direcciones IP:

**`ipv4`**

El balanceador de cargas se comunica con los objetivos mediante. IPv4

**`ipv6`**

El balanceador de cargas se comunica con los objetivos mediante. IPv6

Consideraciones

- El equilibrador de carga se comunica con los destinos en función del tipo de dirección IP del grupo de destino. Los destinos de un grupo IPv4 objetivo deben aceptar el IPv4 tráfico del balanceador de cargas y los destinos de un grupo IPv6 objetivo deben aceptar el IPv6 tráfico del balanceador de cargas.
- No puedes usar un grupo IPv6 objetivo con un balanceador de `ipv4` cargas.
- No puede registrar una función Lambda con un grupo IPv6 objetivo.

# Versión del protocolo

De forma predeterminada, los equilibradores de carga de aplicaciones envían solicitudes a los destinos mediante HTTP/1.1. Puede usar la versión del protocolo para enviar solicitudes a los destinos mediante HTTP/2 o gRPC.

En la siguiente tabla se resumen el resultado de las combinaciones del protocolo de solicitud y la versión del protocolo de grupo de destino.

| Protocolo de solicitud | Versión del protocolo | Resultado |
|---|---|---|
| HTTP/1.1 | HTTP/1.1 | Success |
| HTTP/2 | HTTP/1.1 | Success |
| gRPC | HTTP/1.1 | Error |
| HTTP/1.1 | HTTP/2 | Error |
| HTTP/2 | HTTP/2 | Success |
| gRPC | HTTP/2 | Correcto si los destinos respaldan el gRPC |
| HTTP/1.1 | gRPC | Error |

| Protocolo de solicitud | Versión del protocolo | Resultado |
|---|---|---|
| HTTP/2 | gRPC | Correcto si una solicitud POST |
| gRPC | gRPC | Success |

Consideraciones para la versión del protocolo gRPC

- El único protocolo de oyente compatible es HTTPS.
- El único tipo de acción que se admite para las reglas de oyente es `forward`.
- Solo se admiten los tipos de destino `instance` y `ip`.
- El equilibrador de carga analiza las llamadas de gRPC y las enruta a los grupos de destino adecuados en función del paquete, el servicio y el método.
- El equilibrador de carga admite la transmisión única del lado del cliente, la transmisión del lado del servidor y la transmisión bidireccional.
- Debe proporcionar un método de comprobación de estado personalizado con el formato `/package.service/method`.
- Debe especificar los códigos de estado de gRPC que deben utilizarse al comprobar si se ha recibido una respuesta correcta de un destino.
- No podrá utilizar las funciones de Lambda como destinos.

Consideraciones para la versión del protocolo HTTP/2

- El único protocolo de oyente que se admite es HTTPS.
- El único tipo de acción que se admite para las reglas de oyente es `forward`.
- Solo se admiten los tipos de destino `instance` y `ip`.
- El equilibrador de carga admite la transmisión única del lado del cliente, la transmisión del lado del servidor y la transmisión bidireccional. El número máximo de transmisiones por conexión HTTP/2 de cliente es 128.

# Destinos registrados

El equilibrador 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.

Si aumenta la demanda en la aplicación, puede registrar más destinos en uno o varios grupos para controlar la demanda. El equilibrador de carga comienza a enrutar el tráfico a un destino recién registrado tan pronto como se completa el proceso de registro y el destino supera la primera comprobación de estado inicial, independientemente del umbral configurado.

Si la demanda de la aplicación se reduce o cuando es preciso realizar el mantenimiento de los destinos, puede 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 equilibrador 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 equilibrador de carga con un grupo de escalado automático. Después de asociar un grupo de destino a un grupo de escalado automático, el escalado automático registra los destinos en el grupo de destino cuando los lanza. Para obtener más información, consulte Adjuntar 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 Application Load Balancer en la misma VPC. Si el otro Equilibrador de carga de aplicación está en una VPC que está interconectada a la VPC del equilibrador de carga, puede registrar sus direcciones IP.
- No puedes registrar instancias por ID de instancia si están en una VPC enlazada a la VPC del balanceador de carga (en la misma región o en una región diferente). Puede registrar estas instancias por dirección IP.

# Atributos del grupo de destino

Puede configurar un grupo de destino editando sus atributos. Para obtener más información, consulte Edición de 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.

`load_balancing.algorithm.type`

El algoritmo de equilibrador de carga determina cómo el equilibrador de carga selecciona los destinos al direccionar las solicitudes. El valor es `round_robin`, `least_outstanding_requests` o `weighted_random`. El valor predeterminado es `round_robin`.

`load_balancing.algorithm.anomaly_mitigation`

Solo está disponible cuando `load_balancing.algorithm.type` es `weighted_random`. Indica si la mitigación de anomalías está habilitada. El valor es `on` o `off`. El valor predeterminado es `off`.

`load_balancing.cross_zone.enabled`

Indica si el equilibrio de carga entre zonas está habilitado. El valor es `true`, `false` o `use_load_balancer_configuration`. El valor predeterminado es `use_load_balancer_configuration`.

`slow_start.duration_seconds`

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

`stickiness.enabled`

Indica si están habilitadas las sesiones rápidas. El valor es `true` o `false`. El valor predeterminado es `false`.

`stickiness.app_cookie.cookie_name`

El nombre de la cookie de aplicación. El nombre de la cookie de la aplicación no puede tener los siguientes prefijos:`AWSALB`,`AWSALBAPP`, o`AWSALBTG`; están reservados para que los use el balanceador de cargas.

`stickiness.app_cookie.duration_seconds`

Periodo de vencimiento de las cookies basadas en aplicación, 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.lb_cookie.duration_seconds`

Periodo de vencimiento de las cookies basado en la duración, 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. Los valores posibles son `lb_cookie` y `app_cookie`.

`target_group_health.dns_failover.minimum_healthy_targets.count`

La cantidad mínima de destinos que deben estar en buen estado. Si el número de destinos en buen estado es inferior a este valor, marca el nodo como en mal estado en el DNS para que el tráfico se dirija solo a los nodos en buen estado. Los valores posibles son `off` o un número entero comprendido entre 1 y la cantidad máxima de destinos. Cuando se desactiva el error de DNS`off`, esto significa que, aunque todos los destinos del grupo de destino estén en mal estado, el nodo no se elimina del DNS. El valor predeterminado de es 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

El porcentaje mínimo de destinos que deben estar en buen estado. Si el porcentaje de destinos en buen estado es inferior a este valor, marque el nodo como en mal estado en DNS para que el tráfico se dirija solo a los nodos que están en buen estado. Los valores posibles son `off` o un número entero comprendido entre 1 y 100. Cuando se desactiva el error de DNS`off`, esto significa que, aunque todos los destinos del grupo objetivo estén en mal estado, el nodo no se elimina del DNS. El valor predeterminado es `off`.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

La cantidad mínima de destinos que deben estar en buen estado. Si la cantidad de destinos en buen estado es inferior a este valor, envíe el tráfico a todos los destinos, incluidos los destinos en mal estado. El rango comprende del 1 a la cantidad máxima de destinos. El valor predeterminado de es 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

El porcentaje mínimo de destinos que deben estar en buen estado. Si el porcentaje de destinos en buen estado es inferior a este valor, envíe el tráfico a todos los destinos, incluidos los destinos en mal estado. Los valores posibles son `off` o un número entero comprendido entre 1 y 100. El valor predeterminado es `off`.

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 equilibrador de carga y la función de 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.

## Algoritmos de enrutamiento

Un algoritmo de enrutamiento es el método que utiliza el equilibrador de carga para determinar qué destinos recibirán las solicitudes. De forma predeterminada, el algoritmo de enrutamiento de turno rotativo se utiliza para enviar las solicitudes al nivel del grupo de destino. Las solicitudes menos pendientes y los algoritmos de enrutamiento aleatorio ponderado también están disponibles en función de las necesidades de su aplicación. Un grupo de destino solo puede tener un algoritmo de enrutamiento activo a la vez, sin embargo, el algoritmo de enrutamiento se puede actualizar siempre que sea necesario.

Si habilita sesiones persistentes, se utilizará el algoritmo de enrutamiento seleccionado para seleccionar el destino inicial. Las solicitudes futuras del mismo cliente se reenviarán al mismo destino, sin tener en cuenta el algoritmo de enrutamiento seleccionado.

Turno rotativo

- El algoritmo de enrutamiento de turno rotativo envía las solicitudes de manera uniforme entre los destinos en buen estado del grupo de destino, en orden secuencial.
- Este algoritmo se suele utilizar cuando las solicitudes que se reciben tienen una complejidad similar, los destinos registrados tienen una capacidad de procesamiento similar o si es necesario distribuir las solicitudes por igual entre los destinos.

Solicitudes menos pendientes

- El algoritmo de enrutamiento de las solicitudes menos pendientes envía las solicitudes a los destinos con el menor número de solicitudes en curso.
- Este algoritmo se suele utilizar cuando las solicitudes que se reciben varían en complejidad y los destinos registrados varían en cuanto a su capacidad de procesamiento.
- Cuando un equilibrador de carga que admite HTTP/2 utiliza destinos que únicamente admiten HTTP/1.1, convierte la solicitud en varias solicitudes HTTP/1.1. En esta configuración, el algoritmo de solicitudes menos pendientes tratará cada solicitud HTTP/2 como solicitudes múltiples.
- Cuando se utiliza WebSockets, el destino se selecciona mediante el algoritmo de solicitudes menos pendientes. Una vez seleccionado, el equilibrador de carga crea una conexión con este destino y envía todos los mensajes a través de esta conexión.
- El algoritmo de enrutamiento de solicitudes menos pendientes no se puede usar con el modo de inicio lento.

Aleatorio ponderado

- El algoritmo de enrutamiento aleatorio ponderado envía las solicitudes de manera uniforme entre los destinos en buen estado del grupo de destino, en orden aleatorio.
- Este algoritmo admite la mitigación de anomalías de los pesos de destino automáticos (ATW).
- El algoritmo de enrutamiento aleatorio ponderado no se puede utilizar con el modo de inicio lento.
- El algoritmo de enrutamiento aleatorio ponderado no se puede utilizar con sesiones persistentes.

## Modificación del algoritmo de enrutamiento de un grupo de destino

Puede modificar el algoritmo de enrutamiento del grupo de destino en cualquier momento.

Modificación del algoritmo de enrutamiento mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la página de detalles del grupo de destino, en la pestaña Atributos, seleccione Editar.

5. En la página Editar los atributos del grupo de destino, en la sección Configuración del tráfico, en Algoritmo del equilibrador de carga, seleccione Turno rotativo, Solicitudes menos pendientes o Aleatorio ponderado.
6. Seleccione Save changes (Guardar cambios).

Para modificar el algoritmo de enrutamiento mediante el AWS CLI

Utilice el comando modify-target-group-attributes con el atributo `load_balancing.algorithm.type`.

# Estado del grupo de destino

De forma predeterminada, un grupo de destino se considera en buen estado siempre que tenga al menos un destino en buen estado. Si tiene una flota grande, no basta con tener un solo destino en buen estado que atienda el tráfico. En su lugar, puede especificar un recuento o porcentaje mínimo de destinos que deben estar en buen estado y qué acciones tomará el equilibrador de carga cuando los destinos en buen estado estén por debajo del umbral especificado. Esto mejora la disponibilidad de la aplicación.

Contenido



## Acciones en mal estado

Puede configurar umbrales de buen estado para las siguientes acciones:

- Conmutación por error de DNS: cuando los objetivos en buen estado de una zona están por debajo del umbral, marcamos las direcciones IP del nodo del equilibrador de carga de la zona como en mal estado en el DNS. Por lo tanto, cuando los clientes resuelven el nombre DNS del equilibrador de carga, el tráfico se enruta únicamente a las zonas en buen estado.
- Conmutación por error de enrutamiento: cuando los objetivos en buen estado de una zona están por debajo del umbral, el equilibrador de carga envía tráfico a todos los destinos que

están disponibles para el nodo del equilibrador de carga, incluidos los destinos en mal estado. Esto aumenta las probabilidades de que la conexión de un cliente se realice correctamente, en particular cuando los destinos no pasan temporalmente las comprobaciones de estado, y reduce el riesgo de sobrecargar los destinos en buen estado.

## Requisitos y consideraciones

- Esta característica no se puede utilizar con grupos de destino en los que el destino es una función de Lambda. Si el Equilibrador de carga de aplicación es el destino de un Equilibrador de carga de red o Global Accelerator, no configure un umbral para la conmutación por error de DNS.
- Si especifica ambos tipos de umbrales para una acción (recuento y porcentaje), el equilibrador de carga realizará la acción cuando se supere alguno de los umbrales.
- Si especifica umbrales para ambas acciones, el umbral de la conmutación por error de DNS debe ser mayor o igual que el umbral de la conmutación por error de enrutamiento, de modo que la conmutación por error de DNS se produzca al mismo tiempo que la conmutación por error de enrutamiento o antes.
- Si especifica el umbral como un porcentaje, calculamos el valor de forma dinámica en función de la cantidad total de destinos registrados en los grupos de destino.
- La cantidad total de destinos se basa en si el equilibrio de carga entre zonas está activado o desactivado. Si el equilibrio de carga entre zonas está desactivado, cada nodo envía tráfico solo a los destinos de su propia zona, lo que significa que los umbrales se aplican a la cantidad de destinos de cada zona habilitada por separado. Si el equilibrio de carga entre zonas está activado, cada nodo envía tráfico a todos los destinos de todas las zonas habilitadas, lo que significa que los umbrales especificados se aplican a la cantidad total de destinos de todas las zonas habilitadas. Para obtener más información, consulte Equilibrador de carga entre zonas para los grupos de destino del Equilibrador de carga de aplicación.
- Cuando se produce una conmutación por error de DNS, afecta a todos los grupos de destino asociados al balanceador de cargas. Asegúrese de tener suficiente capacidad en las zonas restantes para gestionar este tráfico adicional, especialmente si el equilibrio de carga entre zonas está desactivado.
- Con la conmutación por error de DNS, eliminamos las direcciones IP de las zonas en mal estado del nombre de host DNS del equilibrador de cargas. Sin embargo, la caché de DNS del cliente local puede contener estas direcciones IP hasta que caduque el time-to-live (TTL) del registro DNS (60 segundos).

- Con la conmutación por error de DNS, si hay varios grupos de destino conectados a un Application Load Balancer y un grupo de destino está en mal estado en una zona, las comprobaciones de estado del DNS se realizan correctamente si al menos otro grupo de destino está en buen estado en esa zona.
- Con la conmutación por error de DNS, si se considera que todas las zonas del equilibrador de carga están en mal estado, el equilibrador de carga envía tráfico a todas las zonas, incluidas las zonas en mal estado.
- Existen otros factores, además de la existencia de suficientes destinos en buen estado, que podrían provocar una conmutación por error de DNS, como el estado de la zona.

## Monitorización

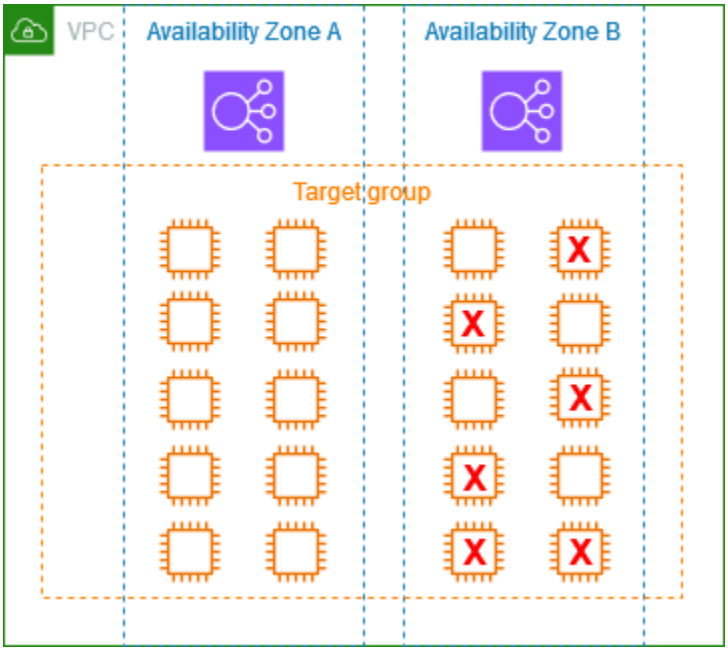
Para supervisar el estado de los grupos objetivo, consulte CloudWatch las métricas del estado del grupo objetivo.

## Ejemplo

En el siguiente ejemplo, se muestra cómo se aplica la configuración de estado del grupo de destino.

Escenario

- Un equilibrador de carga que admite dos zonas de disponibilidad, A y B
- Cada zona de disponibilidad contiene 10 destinos registrados
- El grupo de destino tiene la siguiente configuración de estado del grupo de destino:
  - Conmutación por error de DNS: 50 %
  - Conmutación por error de enrutamiento: 50 %
- Seis destinos fallan en la zona de disponibilidad B




Cuando el equilibrio de carga entre zonas está desactivado

- El nodo del equilibrador de carga de cada zona de disponibilidad solo puede enviar tráfico a los 10 destinos de su zona de disponibilidad.
- Hay 10 destinos en buen estado en la zona de disponibilidad A que cumplen con el porcentaje requerido de destinos en buen estado. El equilibrador de carga sigue distribuyendo el tráfico entre los 10 destinos en buen estado.
- Solo hay 4 destinos en buen estado en la zona de disponibilidad B, es decir, el 40% de los destinos del nodo del equilibrador de carga de la zona de disponibilidad B. Como este porcentaje es inferior al porcentaje de destinos en buen estado requerido, el equilibrador de carga toma las siguientes medidas:
  - Conmutación por error de DNS: la zona de disponibilidad B está marcada como en mal estado en el DNS. Como los clientes no pueden resolver el nombre del equilibrador de carga en el nodo del equilibrador de carga de la zona de disponibilidad B y la zona de disponibilidad A está en buen estado, los clientes envían nuevas conexiones a la zona de disponibilidad A.
  - Conmutación por error de enrutamiento: cuando se envían nuevas conexiones de forma explícita a la zona de disponibilidad B, el equilibrador de carga distribuye el tráfico a todos los destinos de la zona de disponibilidad B, incluidos los destinos en mal estado. Esto evita interrupciones entre los demás destinos en buen estado.

Cuando el equilibrio de carga entre zonas está activado

- Cada nodo del equilibrador de carga puede enviar tráfico a los 20 destinos registrados en ambas zonas de disponibilidad.
- Hay 10 destinos en buen estado en la zona de disponibilidad A y 4 destinos en buen estado en la zona de disponibilidad B, con un total de 14 destinos en buen estado. Esto representa el 70% de los destinos de los nodos del equilibrador de carga en ambas zonas de disponibilidad, lo que cumple con el porcentaje requerido de destinos en buen estado.
- El equilibrador de carga distribuye el tráfico entre los 14 destinos en buen estado en ambas zonas de disponibilidad.

## Uso de la conmutación por error de DNS de Route 53 para el equilibrador de carga

Si utiliza Route 53 para dirigir las consultas de DNS al equilibrador de carga, también puede utilizar Route 53 para configurar la conmutación por error de DNS del equilibrador de carga. En una configuración de conmutación por error, Route 53 comprueba el estado de los destinos del grupo de destino para el equilibrador de carga con el fin de determinar si están disponibles. Si no existen destinos en buen estado registrados en el equilibrador de carga o si este no se encuentra en buen estado, Route 53 enruta el tráfico a otro recurso disponible, como un equilibrador de carga en buen estado o un sitio web estático en Amazon S3.

Por ejemplo, supongamos que tenemos una aplicación web para `www.example.com` y deseamos ejecutar instancias redundantes por detrás de dos equilibradores de carga que residen en regiones distintas. Queremos enrutar el tráfico principalmente al equilibrador de carga de una de las regiones y utilizar el equilibrador de carga de la otra región como copia de seguridad en caso de error. Si configura la conmutación por error de DNS, puede especificar los equilibradores de carga principal y secundario (de copia de seguridad). Route 53 enruta el tráfico al equilibrador de carga principal si está disponible, o bien, en caso contrario, al secundario.

¿Cómo funciona evaluar la salud objetivo

- Si evaluar el estado del objetivo está establecido `Yes` en un registro de alias para un Application Load Balancer, Route 53 evalúa el estado del recurso especificado por el valor. `alias target` Route 53 usa las comprobaciones de estado del grupo objetivo.
- Si todos los grupos de destino asociados a un Application Load Balancer están en buen estado, Route 53 marca el registro de alias como correcto. Si configuró un umbral para un grupo objetivo y

este lo alcanza, pasa las comprobaciones de estado. De lo contrario, si un grupo objetivo contiene al menos un objetivo en buen estado, pasa las comprobaciones de estado. Si se aprueban las comprobaciones de estado, Route 53 devuelve los registros de acuerdo con su política de enrutamiento. Si se utiliza una política de enrutamiento de conmutación por error, Route 53 devuelve el registro principal.

- Si alguno de los grupos de destino adjuntos a un Application Load Balancer está en mal estado, el registro de alias no pasa la comprobación de estado de Route 53 (apertura por error). Si se utiliza la función de evaluación del estado del objetivo, la política de enrutamiento de conmutación por error redirige el tráfico al recurso secundario.
- Si todos los grupos de destino adjuntos a un Application Load Balancer están vacíos (no hay objetivos), Route 53 considera que el registro está en mal estado (se ha abierto por error). Si se utiliza la función de evaluación del estado del objetivo, la política de enrutamiento de conmutación por error redirige el tráfico al recurso secundario.

Para obtener más información, consulte Uso de los umbrales de salud del grupo objetivo del balanceador de carga para mejorar la disponibilidad en el AWS blog y Configuración de la conmutación por error de DNS en la Guía para desarrolladores de Amazon Route 53.

# Creación de un grupo de destino para el Equilibrador de carga de aplicación

Los destinos se registran en un grupo de destino. De forma predeterminada, el equilibrador 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 oyente o crear una regla para este último. Para obtener más información, consulte Reglas del oyente. Puede especificar el mismo grupo de destino en varios oyentes, pero estos oyentes deben pertenecer al mismo Equilibrador de carga de aplicación. Para usar un grupo de destino con un equilibrador de carga, debe comprobar que el grupo de destino no esté siendo utilizado por un oyente para ningún otro equilibrador de carga.

Puede agregar o eliminar destinos del grupo de destino en cualquier momento. Para obtener más información, consulte Registro de destinos con el grupo de destino del Equilibrador de carga de aplicación. También puede modificar la configuración de la comprobación de estado del grupo de

destino. Para obtener más información, consulte Actualización de la configuración de comprobación de estado del grupo de destino de un Equilibrador de carga de aplicación.

Para crear un grupo de destino desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija Crear grupo de destino.
4. En Tipo de destino, seleccione Instancia para registrar los destinos por ID de instancia, IP para registrar direcciones IP y función de Lambda para registrar una función de Lambda.
5. En Target group name, escriba el nombre del nuevo grupo de destino. Este nombre debe ser único por región por cuenta, puede tener un máximo de 32 caracteres, debe contener únicamente caracteres alfanuméricos o guiones y no puede comenzar ni terminar con un guion.
6. (Opcional) En Protocol y Port, modifique los valores predeterminados según sea necesario.
7. Si el tipo de destino es Instancias o direcciones IP, elija IPv4o IPv6como tipo de dirección IP; de lo contrario, pase al siguiente paso.

   Tenga en cuenta que solo los destinos con el tipo de dirección IP seleccionado se pueden incluir en este grupo de destinos. El tipo de dirección IP no se puede cambiar una vez que se creó el grupo de destino.
8. En VPC, seleccione una nube privada virtual (VPC). Tenga en cuenta que, en el caso de los tipos de destino de direcciones IP, los VPCs disponibles para su selección son aquellos que admiten el tipo de dirección IP que eligió en el paso anterior.
9. (Opcional) En Versión del protocolo, modifique los valores predeterminados según sea necesario.
10. (Opcional) En la sección Comprobaciones de estado, mantenga la configuración predeterminada.
11. Si el tipo de destino es la función de Lambda, puede habilitar las comprobaciones de estado seleccionando Habilitar en la sección Comprobaciones de estado.
12. (Opcional) Agregue una o varias etiquetas, como se indica a continuación:

    a. Expanda la sección Etiquetas.

    b. Seleccione Agregar etiqueta.

    c. Escriba la clave y el valor de la etiqueta.

13. Elija Siguiente.
14. (Opcional) Agregue uno o varios destinos, como se indica a continuación:
    - Si el tipo de destino es Instancias, seleccione una o más instancias, introduzca uno o más puertos y, a continuación, elija Incluir como pendiente debajo.

      Nota: Las instancias deben tener una IPv6 dirección principal asignada para poder registrarse en un grupo de IPv6 destino.
    - Si el tipo de destino es direcciones IP, haga lo siguiente:

      a. Seleccione una VPC de red de la lista o elija Otras direcciones IP privadas.

      b. Introduzca la dirección IP manualmente o busque la dirección IP mediante los detalles de la instancia. Puede introducir hasta cinco direcciones IP a la vez.

      c. Introduzca los puertos para enrutar el tráfico a las direcciones IP especificadas.

      d. Seleccione Incluir como pendiente debajo.
    - Si el tipo de destino es una función de Lambda, especifique una sola u omita este paso y especifique una función de Lambda más adelante.
15. Elija Crear grupo de destino.
16. (Opcional) Puede especificar el grupo de destino en una regla de oyente. Para obtener más información, vea Reglas del oyente.

Para crear un grupo objetivo mediante el AWS CLI

Utilice el create-target-groupcomando para crear el grupo objetivo, el comando add-tags para etiquetar el grupo objetivo y el comando register-targets para agregar objetivos.

# Actualización de la configuración de estado del grupo de destino del Equilibrador de carga de aplicación

Puede modificar la configuración del estado de grupo de destino de su grupo de destino de la siguiente manera.

Para modificar la configuración del estado de grupo de destino desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.

3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Compruebe si el equilibrio de carga entre zonas está activado o desactivado. Actualice esta configuración según sea necesario para asegurarse de que tiene suficiente capacidad para gestionar el tráfico adicional en caso de que falle una zona.
6. Amplíe los requisitos de estado del grupo de destino.
7. Para el tipo de configuración, le recomendamos que elija la configuración unificada, que establece el mismo umbral para ambas acciones.
8. Para conocer los requisitos para un buen estado, realice una de las siguientes acciones:
   - Elija Recuento mínimo de destinos en buen estado y, a continuación, introduzca un número entre 1 y el número máximo de destinos para su grupo de destino.
   - Elija el porcentaje mínimo de destinos en buen estado y, a continuación, introduzca un número del 1 al 100.
9. Seleccione Save changes (Guardar cambios).

Para modificar la configuración de salud del grupo objetivo mediante el AWS CLI

Utilice el comando modify-target-group-attributes. En el siguiente ejemplo, se establece el umbral de buen estado para ambas acciones de mal estado en un 50 %.

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067 \
--attributes
 Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \

 Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

# Comprobaciones de estado de los grupos de destinos del Equilibrador de carga de aplicación.

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

Cada nodo del equilibrador de carga direcciona las solicitudes únicamente a los destinos en buen estado de las zonas de disponibilidad habilitadas para el equilibrador de carga. Cada nodo del

equilibrador 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 equilibrador de carga cierra la conexión se estableció para la comprobación de estado.

Si un grupo de destino contiene solo destinos registrados en mal estado, el equilibrador de carga dirige las solicitudes a todos esos destinos, independientemente de su estado. Esto significa que si todos los destinos no pasan las comprobaciones de estado al mismo tiempo en todas las zonas de disponibilidad habilitadas, el equilibrador de carga no se abrirá correctamente. El efecto de la apertura por error es permitir que el tráfico llegue a todos los destinos de todas las zonas de disponibilidad habilitadas, independientemente de su estado, en función del algoritmo de equilibrio de carga.

Los controles de salud no son compatibles WebSockets.

Para obtener más información, consulte the section called “Estado del grupo de destino”.

## Configuración de comprobación de estado

Puede configurar las comprobaciones de estado de los destinos de un grupo de destino según se indica en la siguiente tabla. Los nombres de configuración que se utilizan en la tabla son los que se utilizan en la API. El balanceador de cargas envía una solicitud de comprobación de estado a cada objetivo registrado cada HealthCheckIntervalSecondssegundo, mediante el puerto, el protocolo y la ruta de comprobación de estado especificados. Cada solicitud de comprobación de estado es independiente y el resultado 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 los errores UnhealthyThresholdCountconsecutivos, el equilibrador de cargas deja el objetivo fuera de servicio. Cuando las comprobaciones de estado superan las HealthyThresholdCountcorrectas consecutivas, el equilibrador de cargas vuelve a poner el objetivo en servicio.

Ten en cuenta que cuando cancelas el registro de un objetivo, este porcentaje disminuye HealthyHostCountpero no aumenta. UnhealthyHostCount

| Opción | Descripción |
| --- | --- |
| HealthCheckProtocol | Protocolo que el equilibrador de carga utiliza al realizar comprobaciones de estado en |

| Opción | Descripción |
| --- | --- |
| | los destinos. Para Equilibradores de carga de aplicación, los protocolos admitidos son HTTP y HTTPS. El valor predeterminado es el protocolo HTTP.<br><br>Estos protocolos utilizan el método HTTP GET para enviar las solicitudes de comprobación de estado. |
| HealthCheckPort | Puerto que el equilibrador 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 equilibrador de carga. |
| HealthCheckPath | El destino para las comprobaciones de estado en los destinos.<br><br>Si la versión del protocolo es HTTP/1.1 o HTTP/2, especifique un URI válido (/ruta?consulta). El valor predeterminado es /.<br><br>Si la versión del protocolo es gRPC, especifiq ue la ruta del método de comprobación de estado personalizado con el formato `/package.service/method` . El valor predeterminado es `/AWS.ALB/healthche ck` . |
| HealthCheckTimeoutSeconds | Cantidad de tiempo, en segundos, durante la cual ninguna respuesta de un destino significa una comprobación de estado fallida. El rango va de 2 a 120 segundos. El valor predeterm inado es 5 segundos si el tipo de destino es `instance` o `ip` y 30 segundos si el tipo de destino es `lambda`. |

| Opción | Descripción |
| --- | --- |
| 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 30 segundos si el tipo de destino es `instance` o `ip` y 35 segundos si el tipo de destino es `lambda`. |
| 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. |

| Opción | Descripción |
| --- | --- |
| Matcher | Códigos que se deben utilizar al comprobar si se ha recibido una respuesta exitosa de un destino. En la consola, se denominan códigos de éxito.<br><br>Si la versión del protocolo es HTTP/1.1 o HTTP/2, los valores posibles oscilan entre 200 y 499. Puede especificar varios valores (por ejemplo, “200,202”) o un intervalo de valores (por ejemplo, “200-299”). El valor predeterm inado es 200.<br><br>Si la versión del protocolo es gRPC, los valores posibles van de 0 a 99. Puede especific ar varios valores (por ejemplo, “0,1”) o un intervalo de valores (por ejemplo, “0-5”). El valor predeterminado es 12. |

## Estado del destino

Antes de que el equilibrador 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 oyente y asegurarse de que la zona de disponibilidad del destino esté habilitada en el equilibrador de carga. Para que un destino pueda recibir solicitudes desde el equilibrador 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 equilibrador de carga se encuentra en proceso de registrar el destino o de realizar las comprobaciones de estado iniciales en el destino. |

| Valor | Descripción |
| --- | --- |
| | Códigos de motivo relacionados: `Elb.RegistrationInProgress` \| `Elb.InitialHealthChecking` |
| `healthy` | El destino se encuentra en buen estado.<br><br>Códigos de motivo relacionados: ninguno |
| `unhealthy` | El destino no respondió a una comprobación de estado o no la ha superado.<br><br>Códigos de motivo relacionados: `Target.ResponseCodeMismatch` \| `Target.Timeout` \| `Target.FailedHealthChecks` \| `Elb.InternalError` |
| `unused` | El destino no está registrado en un grupo de destino, el grupo de destino no se utiliza en una regla del oyente, el destino se encuentra en una zona de disponibilidad que no está habilitada o el destino está en un estado detenido o terminado.<br><br>Códigos de motivo relacionados: `Target.NotRegistered` \| `Target.NotInUse` \| `Target.InvalidState` \| `Target.IpUnusable` |
| `draining` | El destino está en proceso de anulación del registro y de vaciado de conexiones.<br><br>Código de motivo relacionado: `Target.DeregistrationInProgress` |
| `unavailable` | Las comprobaciones de estado están deshabilitadas para el grupo de destino.<br><br>Código de motivo relacionado: `Target.HealthCheckDisabled` |

# 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, y la consola muestra la misma descripción. Los códigos de motivo que comienzan por `Elb` tienen su origen en el equilibrador de carga y que los códigos de motivo que comienzan por `Target` tienen su origen en el destino. Para obtener más información sobre las posibles causas de los errores en las comprobaciones de estado, consulte Solución de problemas.

| 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.HealthCheckDisabled` | Las comprobaciones de estado están deshabilitadas |
| `Target.InvalidState` | El destino se encuentra en estado detenido.<br>El destino se encuentra en estado terminado.<br>El destino se encuentra en estado terminado o detenido.<br>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 equilibrador de carga. |

| Código de motivo | Descripción |
| --- | --- |
| | El destino se encuentra en una zona de disponibilidad que no está habilitada para el equilibrador 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 del Equilibrador de carga de aplicación

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

Para comprobar el estado de los destinos desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Seleccione el nombre del grupo de destino para abrir la página de detalles.
4. En la pestaña Targets la Status columna indica el estado de cada destino.
5. Si el estado es un valor distinto de `Healthy`, la columna Detalles del estado contiene más información. Para obtener ayuda con los errores en las comprobaciones de estado, consulte Solución de problemas.

Para comprobar el estado de tus objetivos, utiliza el 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.

Para recibir notificaciones por correo electrónico sobre destinos en mal estado

Utilice CloudWatch alarmas para activar una función Lambda que envíe detalles sobre objetivos en mal estado. Para step-by-step obtener instrucciones, consulta la siguiente entrada del blog: Cómo identificar los objetivos insalubres de tu balanceador de cargas.

## Actualización de la configuración de comprobación de estado del grupo de destino de un Equilibrador de carga de aplicación

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

Actualización de la configuración de comprobación de estado de un grupo de destino desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Configuración de comprobación de estado, seleccione Editar.
5. En la página Editar la configuración de la comprobación de estado, modifique la configuración según sea necesario y, a continuación, seleccione Guardar cambios.

Para modificar la configuración de los controles de estado de un grupo objetivo mediante el AWS CLI

Utilice el comando modify-target-group.

# Edición de los atributos del grupo de destino del Equilibrador de carga de aplicación

Después de crear un grupo de destino para el Equilibrador de carga de aplicación, puede editar los atributos del grupo de destino.

Atributos del grupo de destino

- Retardo de anulación del registro
- Modo de inicio lento

- Equilibrador de carga entre zonas para los grupos de destino del Equilibrador de carga de aplicación
- Pesos de destino automáticos (ATW)
- Sesiones persistentes para Equilibrador de carga de aplicación

## Retardo de anulación del registro

Elastic Load Balancig 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 escalado automático, 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. Una vez transcurrido el tiempo de espera, el destino pasa a un estado `unused`.

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. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Editar atributos, cambie el valor de Retardo de anulación de registro según sea necesario.

6. Seleccione Save changes (Guardar cambios).

Para actualizar el valor del retraso en la cancelación del registro mediante el 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 equilibrador de carga les envíe una cuota completa de solicitudes.

Después de habilitar el inicio lento para un grupo de destino, sus destinos entran en modo de inicio lento cuando el grupo de destino los considera en buen estado. Un destino en modo de inicio lento sale de este modo cuando transcurre el período de duración de inicio lento configurado o el destino deja de estar en buen estado. El equilibrador de carga aumenta linealmente el número de solicitudes que puede enviar a un destino en modo de inicio lento. Una vez que un destino en buen estado sale del modo de inicio lento, el equilibrador de carga puede enviarle una cuota completa de solicitudes.

Consideraciones

- Al habilitar el inicio lento para un grupo de destino, los destinos en buen estado registrados en 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 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 en buen estado 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 vuelve a registrar el mismo destino, este entra en modo de inicio lento cuando el grupo de destino lo considere en buen estado.
- Si un destino en modo de inicio lento dejar de estar en buen estado, el destino sale del modo de inicio lento. Cuando el destino está en buen estado, este vuelve a entrar en el modo de inicio lento.
- No se puede activar el modo de inicio lento cuando se utilizan las solicitudes menos pendientes o los algoritmos de enrutamiento aleatorio ponderado.

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

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Editar atributos, cambie el valor de Duración de inicio lento según sea necesario y, a continuación, seleccione Guardar. Para deshabilitar el modo de inicio lento, establezca la duración en 0.
6. Seleccione Save changes (Guardar cambios).

Para actualizar el valor de duración del inicio lento utilizando el AWS CLI

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

## Equilibrador de carga entre zonas para los grupos de destino del Equilibrador de carga de aplicación

Los nodos del equilibrador de carga distribuyen las solicitudes procedentes de los clientes entre los destinos registrados. Cuando el equilibrio de carga entre zonas está habilitado, cada nodo del equilibrador de carga distribuye el tráfico entre los destinos registrados de todas las zonas de disponibilidad habilitadas. Cuando el equilibrio de carga entre zonas está deshabilitado, cada nodo del equilibrador de carga distribuye el tráfico únicamente entre los destinos registrados de su zona de disponibilidad. Esto puede ser si se prefieren los dominios de fallos zonales en lugar de los regionales, para garantizar que una zona en buen estado no se vea afectada por una zona en mal estado o para mejorar la latencia general.

Con los equilibradores de carga de aplicaciones, el equilibrio de carga entre zonas siempre está activado en el nivel del equilibrador de carga y no se puede desactivar. Para los grupos de destino, la configuración del equilibrador de carga está predeterminada, pero puede anularla activando o desactivando explícitamente el equilibrio de carga entre zonas al nivel del grupo de destino.

Consideraciones

- La pertinencia de destino no está adminitda cuando equilibrio de carga entre zonas está deshabilitado.

- Las funciones de Lambda como destinos no son admitidos cuando un equilibrador de carga entre zonas está deshabilitado.
- Si se intenta desactivar el equilibrio de carga entre zonas a través de la API de `ModifyTargetGroupAttributes`, si los destinos tienen `AvailabilityZone` de parámetros establecidos en resultados de `all` en un error.
- Al registrar los destinos, el parámetro de `AvailabilityZone` es obligatorio. Después de crear un equilibrador de carga entre zonas en cualquier momento, el equilibrio de carga entre zonas está deshabilitado. De lo contrario, el parámetro se ignora y se trata como `all`.

Prácticas recomendadas

- Planifique una capacidad de destino suficiente en todas las zonas de disponibilidad que prevé utilizar, por grupo de destino. Si no puede planificar una capacidad suficiente en todas las zonas de disponibilidad participantes, recomendamos que mantenga activado el equilibrio de carga entre zonas.
- Al configurar su Equilibrador de carga de aplicación con varios grupos de destino, asegúrese de que todos los grupos de destino participen en las mismas zonas de disponibilidad, dentro de la región configurada. Esto evita que una zona de disponibilidad quede vacía mientras el equilibrio de carga entre zonas esté desactivado, ya que provoca un error 503 en todas las solicitudes HTTP que entran en la zona de disponibilidad vacía.
- Evite crear subredes vacías. Los equilibradores de carga de aplicaciones exponen las direcciones IP de zona a través del DNS para las subredes vacías, lo que desencadena errores 503 en las solicitudes HTTP.
- En algunos casos, un grupo de destino con el equilibrio de carga entre zonas desactivado tiene una capacidad de destino planificada suficiente por zona de disponibilidad, pero todos los destinos de una zona de disponibilidad dejan de funcionar correctamente. Cuando hay al menos un grupo de destino con todos los destinos en un estado, las direcciones IP de los nodos del equilibrador de carga se eliminan del DNS. Cuando el grupo de destino tiene al menos un destino en buen estado, las direcciones IP se restauran en el DNS.

## Deshabilitar el equilibrio de carga entre zonas

Puede deshabilitar un equilibrador de carga entre zonas para sus grupos de destino del Equilibrador de carga de aplicación en cualquier momento.

Para deshabilitar el equilibrio de carga entre zonas desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el nombre del grupo de destino para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar los atributos del grupo de destino, seleccione Deshabilitar para el equilibrio de carga entre zonas.
6. Seleccione Save changes (Guardar cambios).

Para desactivar el equilibrio de carga entre zonas mediante el AWS CLI

Utilice el modify-target-group-attributescomando y defina `false` el `load_balancing.cross_zone.enabled` atributo en.

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=false
```

A continuación, se muestra un ejemplo de respuesta:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "false"
        },
    ]
}
```

## Habilitar equilibrio de carga entre zonas

Puede habilitar un equilibrador de carga entre zonas para sus grupos de destino del Equilibrador de carga de aplicación en cualquier momento. La configuración del equilibrio de carga entre zonas a nivel del grupo de destino anula la configuración a nivel del equilibrador de carga.

Para habilitar el equilibrio de carga entre zonas desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.

3. Seleccione el nombre del grupo de destino para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar los atributos del grupo de destino, seleccione Habilitar para el equilibrio de carga entre zonas.
6. Seleccione Save changes (Guardar cambios).

Para activar el balanceo de carga entre zonas mediante el AWS CLI

Utilice el modify-target-group-attributescomando y defina `true` el `load_balancing.cross_zone.enabled` atributo en.

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=true
```

A continuación, se muestra un ejemplo de respuesta:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "true"
        },
    ]
}
```

## Pesos de destino automáticos (ATW)

Los pesos de destino automáticos (ATW) supervisan constantemente los destinos en los que se ejecutan sus aplicaciones y detectan desviaciones de rendimiento significativas, conocidas como anomalías. Los ATW permiten ajustar dinámicamente la cantidad de tráfico que se enruta a los destinos mediante la detección de anomalías en los datos en tiempo real.

Los pesos de destino automáticos (ATW) detectan automáticamente las anomalías en todos los Equilibradores de carga de aplicación de la cuenta. Cuando se identifican destinos anómalos, ATW pueden intentar estabilizarlos automáticamente; para ello, reducen la cantidad de tráfico a los que se enrutan, lo que se conoce como mitigación de anomalías. ATW optimizan continuamente la distribución del tráfico para maximizar las tasas de éxito por destino y, al mismo tiempo, minimizar las tasas de error del grupo de destino.

Consideraciones:

- La detección de anomalías supervisa actualmente los códigos de respuesta HTTP 5xx que provienen de sus destinos y los errores de conexión que se producen en ellos. La detección de anomalías está siempre activada y no se puede desactivar.
- No se admite ATW cuando se utiliza Lambda como destino.

## Detección de anomalías

La detección de anomalías de ATW supervisa cualquier destino que muestre una desviación significativa en su comportamiento en comparación con otros destinos de su grupo de destino. Estas desviaciones, denominadas anomalías, se determinan al comparar el porcentaje de errores de un destino con el porcentaje de errores de otros destinos del grupo de destino. Estos errores pueden ser tanto errores de conexión como códigos de error HTTP. Los destinos que devuelven cifras significativamente más altas que sus pares se consideran anómalos.

La detección de anomalías requiere un mínimo de tres destinos en buen estado en el grupo de destino. Cuando un destino está registrado en un grupo de destino, primero tiene que pasar las comprobaciones de estado para empezar a recibir tráfico. Una vez que el destino recibe tráfico, ATW comienza a supervisarlo y publica continuamente el resultado de la anomalía. En el caso de los destinos sin anomalías, el resultado de la anomalía es `normal`. En el caso de los destinos con anomalías, el resultado de la anomalía es `anomalous`.

La detección de anomalías de ATW funciona de forma independiente a las comprobaciones de estado del grupo de destino. Un destino puede superar todas las comprobaciones de estado del grupo de destino, pero aun así puede marcarse como anómalo debido a una elevada tasa de error. El hecho de que los destinos pasen a ser anómalos no afecta al estado de las comprobaciones de estado del grupo de destino.

Estado de detección de anomalías

ATW publica continuamente el estado de las detecciones de anomalías que realiza en los destinos. Puede ver el estado actual en cualquier momento con la tecla AWS Management Console o AWS CLI.

Visualización del estado de detección de anomalías mediante la consola

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

2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la página de detalles del grupo de destino, seleccione la pestaña Destinos.
5. En la tabla Destinos registrados, puede ver el estado de las anomalías de cada destino en la columna Resultado de la detección de anomalías.

   Si no se detectó ninguna anomalía, el resultado es `normal`.

   Si se detectaron anomalías, el resultado es `anomalous`.

Para ver los resultados de la detección de anomalías mediante el AWS CLI

Utilice el describe-target-healthcomando con el valor del `Include.member.N` atributo establecido en. `AnomalyDetection`

## Mitigación de anomalías

> **Important**
>
> La función de mitigación de anomalías de ATW solo está disponible cuando se utiliza el algoritmo de enrutamiento aleatorio ponderado.

La mitigación de anomalías de ATW desvía automáticamente el tráfico de los destinos anómalos, lo que les da la oportunidad de recuperarse.

Durante la mitigación:

- ATW ajusta periódicamente la cantidad de tráfico que se enruta a destinos anómalos. Actualmente, el período es cada cinco segundos.
- ATW reduce la cantidad de tráfico que se dirige a destinos anómalos al mínimo necesario para mitigar las anomalías.
- En el caso de los destinos que ya no se detectan como anómalos, se les enrutará más tráfico gradualmente hasta que alcancen la paridad con otros destinos normales del grupo de destino.

### Activación de la mitigación de anomalías de ATW

Puede activar la mitigación de anomalías en cualquier momento.

#### Activación de la mitigación de anomalías mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la página de detalles del grupo de destino, en la pestaña Atributos, seleccione Editar.
5. En la página Editar los atributos del grupo de destino, en la sección Configuración del tráfico, en Algoritmo del equilibrador de carga, asegúrese de que esté seleccionada la opción Aleatorio ponderado.

   Nota: Cuando se selecciona inicialmente el algoritmo aleatorio ponderado, la detección de anomalías está activada de forma predeterminada.
6. En Mitigación de anomalías, asegúrese de que esté seleccionada la opción Encender la mitigación de anomalías.
7. Seleccione Save changes (Guardar cambios).

#### Para activar la mitigación de anomalías mediante el AWS CLI

Utilice el comando modify-target-group-attributes con el atributo `load_balancing.algorithm.anomaly_mitigation`.

### Estado de mitigación de anomalías

Siempre que ATW esté realizando una mitigación en un objetivo, puedes ver el estado actual en cualquier momento con la AWS Management Console tecla o. AWS CLI

#### Visualización del estado de la mitigación de anomalías mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.

4. En la página de detalles del grupo de destino, seleccione la pestaña Destinos.
5. En la tabla de Destinos registrados, puede ver el estado de mitigación de las anomalías de cada destino en la columna Mitigación activa.

   Si la mitigación no está en curso, el estado es `yes`.

   Si la mitigación está en curso, el estado es `no`.

Para ver el estado de mitigación de anomalías mediante el AWS CLI

Utilice el describe-target-healthcomando con el valor del `Include.member.N` atributo establecido en. `AnomalyDetection`

## Sesiones persistentes para Equilibrador de carga de aplicación

De forma predeterminada, un Equilibrador de carga de aplicación enruta cada solicitud de manera independiente a un destino registrado en función del algoritmo de equilibrio de carga elegido. Sin embargo, puede utilizar la característica de sesión persistente (también denominada afinidad de sesión) que permite que el equilibrador de carga vincule una sesión del usuario a una instancia concreta. Con ello se garantiza que todas las solicitudes de ese usuario durante la sesión se envían al mismo destino. Esta característica resulta útil para los servidores que mantienen información de estado, para ofrecer una experiencia de continuidad a los clientes. Para utilizar las sesiones persistentes, los clientes deben admitir las cookies.

Los equilibradores de carga de aplicaciones admiten cookies basadas en la duración y cookies basadas en aplicaciones. Las sesiones persistentes se habilitan para grupos de destino. Se puede usar una combinación de persistencia en función de la duración, persistencia en función de la aplicación y ausencia de persistencia en los grupos de destino.

La clave para administrar las sesiones persistentes consiste en determinar durante cuánto tiempo deberá direccionar el equilibrador de carga la solicitud del usuario a la misma instancia. Si la aplicación tiene su propia cookie de sesión, entonces puede usar la persistencia en función de la aplicación y la cookie de sesión del equilibrador de carga respeta la duración especificada por la cookie de sesión de la aplicación. Si la aplicación no tiene su propia cookie de sesión, entonces puede utilizar la persistencia en función de la duración para generar una cookie de sesión del equilibrador de carga con una duración especificada.

El contenido de estas cookies generadas por el equilibrador de carga se cifra mediante una clave rotativa. No puedes descifrar ni modificar las cookies generadas por el balanceador de cargas.

Para ambos tipos de persistencia, el Equilibrador de carga de aplicación restablece la caducidad de las cookies que genera después de cada solicitud. Si una cookie caduca, la sesión deja de ser persistente y el cliente debe eliminarla de su almacén de cookies.

Requisitos

- Un equilibrador de HTTP/HTTPS carga.
- Al menos una instancia en buen estado en cada zona de disponibilidad.

Consideraciones

- Las sesiones persistentes no son compatibles si el equilibrio de carga entre zonas está deshabilitado. Si se intentan habilitar sesiones persistentes con el equilibrio de carga entre zonas deshabilitado, se producirá un error.
- En el caso de las cookies basadas en aplicaciones, los nombres de las cookies deben especificarse individualmente para cada grupo de destino. Sin embargo, en el caso de las cookies basadas en la duración, `AWSALB` es el único nombre que se utiliza en todos los grupos de destino.
- Si se utilizan varios niveles de equilibradores de carga de aplicaciones, puede habilitar sesiones persistentes en todas las capas con cookies basadas en aplicaciones. Sin embargo, con las cookies basadas en la duración, solo puede habilitar las sesiones persistentes en una capa, ya que `AWSALB` es el único nombre disponible.
- Si el Equilibrador de carga de aplicación recibe `AWSALBCORS` y una cookie de persistencia basada en la duración `AWSALB`, prevalecerá el valor en `AWSALBCORS`.
- La persistencia en función de aplicaciones no funciona con grupos de destino ponderados.
- Si tiene una acción de reenvío con varios grupos de destino y uno o más de ellos tienen habilitadas las sesiones persistentes, debe habilitar la persistencia en el nivel del grupo de destino.
- WebSocket las conexiones son intrínsecamente pegajosas. Si el cliente solicita una actualización de la conexión WebSockets, el destino que devuelve un código de estado HTTP 101 para aceptar la actualización de la conexión es el destino utilizado en la WebSockets conexión. Una vez completada la WebSockets actualización, no se utiliza la adherencia basada en cookies.
- Los equilibradores de carga de aplicaciones utilizan el atributo `Expires` del encabezado de la cookie en lugar del atributo `Max-Age`.
- Los equilibradores de carga de aplicaciones no admiten valores de cookies codificados como URL.
- Si el Application Load Balancer recibe una nueva solicitud mientras el destino se está agotando debido a la cancelación del registro, la solicitud se redirige a un destino en buen estado.

## Persistencia en función de la duración

La rigidez en función de la duración dirige las solicitudes al mismo destino de un grupo de destino mediante una cookie generada por el equilibrador de carga (`AWSALB`). La cookie se utiliza para asignar la sesión al destino. Si la aplicación no tiene su propia cookie de sesión, puede especificar su propia duración de persistencia y administrar durante cuánto tiempo el equilibrador de carga debe dirigir de manera consistente la solicitud del usuario al mismo destino.

Cuando un equilibrador de carga recibe una solicitud de un cliente por primera vez, la direcciona a un destino (según el algoritmo seleccionado) y genera una cookie denominada `AWSALB`. Codifica la información sobre el destino seleccionado, cifra la cookie y la incluye en la respuesta al cliente. La cookie generada por el equilibrador de carga tiene su propia caducidad de 7 días, que no se puede configurar.

En las solicitudes posteriores, el cliente debe incluir la cookie `AWSALB`. Cuando el equilibrador de carga recibe una solicitud de un cliente que contiene la cookie, la detecta y dirige la solicitud al mismo destino. Si la cookie está presente pero no se puede decodificar, o si se refiere a un destino que se ha dado de baja o no está en buen estado, el balanceador de cargas selecciona un nuevo destino y actualiza la cookie con información sobre el nuevo destino.

Para las solicitudes CORS (intercambio de recursos de varios orígenes), algunos navegadores requieren `SameSite=None; Secure` para habilitar la persistencia. Para admitir esos navegadores, el equilibrador de carga siempre genera una segunda cookie de persistencia, `AWSALBCORS`, que incluye la misma información que la cookie de persistencia original, además del atributo `SameSite`. Los clientes reciben ambas cookies, incluidas las solicitudes que no son de CORS.

Para habilitar la persistencia en función de la duración mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Edit attributes, lleve a cabo alguna de las siguientes operaciones:
    a. Seleccione Persistencia.
    b. Para Tipo de persistencia, seleccione Cookie generada por el equilibrador de carga.

c. Para Duración de la persistencia, especifique un valor comprendido entre 1 segundo y 7 días.

d. Seleccione Save changes (Guardar cambios).

Para habilitar la adherencia basada en la duración, utilice la AWS CLI

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

Use el siguiente comando para habilitar la persistencia en función de la duración.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true
 Key=stickiness.lb_cookie.duration_seconds,Value=time-in-seconds
```

El resultado debería ser similar al siguiente ejemplo.

```
    {
       "Attributes": [
          ...
           {
                "Key": "stickiness.enabled",
                "Value": "true"
             },
             {
                 "Key": "stickiness.lb_cookie.duration_seconds",
                 "Value": "86500"

             },
          ...
        ]
     }
```

## Persistencia en función de la aplicación

La persistencia en función de la aplicación le brinda la flexibilidad de establecer sus propios criterios para determinar la persistencia a los destinos del cliente. Cuando se habilita la persistencia en función de las aplicaciones, el equilibrador de carga dirige la primera solicitud a un destino del grupo de destino en función del algoritmo elegido. Se espera que el destino establezca una cookie de aplicación personalizada que coincida con la cookie configurada en el equilibrador de carga para

permitir la persistencia. Esta cookie personalizada puede incluir cualquiera de los atributos de cookie requeridos por la aplicación.

Cuando el Equilibrador de carga de aplicación recibe la cookie de aplicación personalizada del destino, genera automáticamente una nueva cookie de aplicación cifrada para capturar la información de persistencia. Esta cookie de aplicación generada por el equilibrador de carga captura la información sobre la persistencia de cada grupo de destino que tiene habilitada la persistencia en función de aplicaciones.

La cookie de aplicación generada por el equilibrador de carga no copia los atributos de la cookie personalizada establecida por el destino. Tiene su propia caducidad de 7 días, que no se puede configurar. En la respuesta al cliente, el Equilibrador de carga de aplicación solo valida el nombre con el que se configuró la cookie personalizada a nivel del grupo de destino y no el valor ni el atributo de caducidad de la cookie personalizada. Siempre que el nombre coincida, el equilibrador de carga envía ambas cookies, la cookie personalizada establecida por el destino y la cookie de aplicación generada por el equilibrador de carga, en la respuesta al cliente.

En las solicitudes posteriores, los clientes tienen que devolver ambas cookies para mantener la persistencia. El equilibrador de carga descifra la cookie de la aplicación y comprueba si el tiempo de permanencia configurado sigue siendo válido. Luego, utiliza la información de la cookie para enviar la solicitud al mismo destino dentro del grupo de destino con el fin de mantener la persistencia. El equilibrador de carga también envía por proxy la cookie de la aplicación personalizada al destino sin inspeccionarla ni modificarla. En las respuestas posteriores, se restablecen la fecha de caducidad de la cookie de aplicación generada por el equilibrador de carga y el tiempo de permanencia configurado en el equilibrador de carga. Para mantener la persistencia entre el cliente y el destino, la caducidad de la cookie y el tiempo de persistencia no deben llegar a su fin.

Si se produce un error en una instancia o esta pasa a encontrarse en mal estado, el equilibrador de carga deja de enrutar las solicitudes a esa instancia y elige una nueva en buen estado en función del algoritmo de equilibrio de carga existente. El equilibrador de carga trata la sesión como si estuviera “adherida” a la nueva instancia en buen estado y continúa direccionando las solicitudes a esa instancia aunque la instancia que sufrió el error vuelva a estar en buen estado.

En el caso de las solicitudes de intercambio de recursos entre orígenes (CORS), el equilibrador de carga añade los atributos `SameSite=None; Secure` a la cookie de la aplicación generada por el equilibrador de carga solo si la versión del agente de usuario es Chromium80 o superior.

Debido a que la mayoría de los navegadores limitan una cookie a 4 KB de tamaño, el equilibrador de carga fragmenta las cookies de más de 4 KB en varias cookies. Los equilibradores de carga

de aplicaciones admiten cookies de hasta 16 KB y, por lo tanto, pueden crear hasta 4 particiones para enviarlos al cliente. El nombre de la cookie de la aplicación que ve el cliente comienza por «AWSALBAPP-» e incluye un número de fragmento. Por ejemplo, si el tamaño de la cookie es de 0 a 4 K, el cliente ve AWSALBAPP -0. Si el tamaño de la cookie es de 4 a 8 k, el cliente ve AWSALBAPP -0 y -1, y AWSALBAPP así sucesivamente.

Para habilitar las sesiones persistentes controladas por la aplicación desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Edit attributes, lleve a cabo alguna de las siguientes operaciones:

    a. Seleccione Persistencia.
    b. Para el tipo de persistencia, seleccione Cookie en función de aplicaciones.
    c. Para Duración de la persistencia, especifique un valor comprendido entre 1 segundo y 7 días.
    d. En Nombre de la cookie de la aplicación, ingrese un nombre para la cookie en función de la aplicación.

        No utilice `AWSALB`, `AWSALBAPP` o `AWSALBTG` para el nombre de la cookie; están reservados para el uso del equilibrador de carga.
    e. Seleccione Save changes (Guardar cambios).

Para habilitar la adherencia basada en aplicaciones, utilice el AWS CLI

Utilice el modify-target-group-attributescomando con los siguientes atributos:

- `stickiness.enabled`
- `stickiness.type`
- `stickiness.app_cookie.cookie_name`
- `stickiness.app_cookie.duration_seconds`

Use el siguiente comando para habilitar la persistencia en función de aplicaciones.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true Key=stickiness.type,Value=app_cookie
 Key=stickiness.app_cookie.cookie_name,Value=my-cookie-name
 Key=stickiness.app_cookie.duration_seconds,Value=time-in-seconds
```

El resultado debería ser similar al siguiente ejemplo.

```
      {
           "Attributes": [
               ...
               {
                   "Key": "stickiness.enabled",
                   "Value": "true"
               },
               {
                   "Key": "stickiness.app_cookie.cookie_name",
                   "Value": "MyCookie"
               },
               {
                   "Key": "stickiness.type",
                   "Value": "app_cookie"
               },
               {
                   "Key": "stickiness.app_cookie.duration_seconds",
                   "Value": "86500"
               },
               ...
           ]
       }
```

Reequilibrado manual

Al escalar verticalmente, si el número de destinos aumenta considerablemente, existe la posibilidad de que la carga se distribuya de forma desigual debido a la persistencia. En este escenario, puede reequilibrar la carga sobre los destinos mediante las dos opciones siguientes:

- Establezca un vencimiento en la cookie generada por la aplicación que sea anterior a la fecha y la hora en curso. Esto evitará que los clientes envíen la cookie al Equilibrador de carga de aplicación, lo que reiniciará el proceso de establecimiento de la persistencia.

- Establezca una duración muy corta en la configuración de persistencia en función de aplicaciones del equilibrador de carga, por ejemplo, 1 segundo. Esto obliga al Equilibrador de carga de aplicación a restablecer la persistencia incluso si la cookie establecida por el destino no ha caducado.

# Registro de destinos con el grupo de destino del Equilibrador de carga de aplicación

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 instancias IDs, direcciones IP o funciones Lambda. Para obtener más información, consulte Grupos de destino para los equilibradores de carga de aplicaciones.

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 equilibrador 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 equilibrador 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 equilibrador 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 destino 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 equilibrador de carga con un grupo de escalado automático. Después de asociar un grupo de destino a un grupo de escalado automático y cuando el grupo escala horizontalmente, las instancias lanzadas por el grupo de escalado automático se registran automáticamente en el grupo de destino. Si separa el grupo de destino del grupo de escalado automático, automáticamente se anula el registro de las instancias en el grupo de destino. Para obtener más información, consulte Adjuntar un balanceador de carga a su grupo de Auto Scaling en la Guía del usuario de Amazon EC2 Auto Scaling.

Al cerrar una aplicación en un destino, primero debe anular el registro del objetivo de su grupo objetivo y dejar tiempo para que se agoten las conexiones existentes. Puede supervisar el estado de anulación del registro mediante el comando describe-target-health CLI o actualizando la vista del grupo objetivo en el. AWS Management Console Tras confirmar que el objetivo se ha dado de baja, puede continuar con la detención o el cierre de la aplicación. Esta secuencia evita que los usuarios experimenten errores del orden del 50% al cerrar las aplicaciones mientras se sigue procesando el tráfico.

## Grupos de seguridad de destino

Al registrar EC2 las instancias como destinos, debe asegurarse de que los grupos de seguridad de las instancias permitan que el balanceador de carga se comunique con las instancias tanto en el puerto de escucha como en el puerto de comprobación de estado.

Reglas recomendadas

Inbound

| Source | Port Range | Comment |
| --- | --- | --- |
| *load balancer security group* | *instance listener* | Permite el tráfico del equilibrador de carga en el puerto del oyente de la instancia |
| *load balancer security group* | *health check* | Permitir el tráfico procedente del equilibrador 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 Path MTU Discovery en la Guía del EC2 usuario de Amazon.

## Subredes compartidas

Los participantes pueden crear un Equilibrador de carga de aplicación en una VPC compartida. Los participantes no pueden registrar un destino que se ejecute en una subred que no esté compartida con ellos.

# Registro o anulación del registro 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.

Contenido



## Registro o anulación del registro de destinos por ID de instancia

> **Note**
>
> Al registrar los objetivos por ID de instancia para un grupo de IPv6 objetivos, los objetivos deben tener una IPv6 dirección principal asignada. Para obtener más información, consulta IPv6 las direcciones en la Guía del EC2 usuario de Amazon

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

Para registrar un destino o anular su registro mediante el ID de instancia desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Para registrar instancias, elija Registrar destinos. Seleccione una o más instancias, ingrese el puerto de instancia predeterminado según sea necesario y, a continuación, elija Incluir como pendiente debajo. Cuando haya terminado de agregar instancias, elija Registrar destinos pendientes.

   Nota:

- Las instancias deben tener una IPv6 dirección principal asignada para poder registrarse en un grupo IPv6 objetivo.
- AWS GovCloud (US) Region Los s no admiten la asignación de una IPv6 dirección principal mediante la consola. Debes usar la API para asignar IPv6 direcciones principales en AWS GovCloud (US) Region s.

6. Para anular el registro de instancias, seleccione la instancia y, a continuación, elija Anular registro.

## Registro o anulación del registro de destinos por dirección IP

IPv4 objetivos

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)

No puede registrar las direcciones IP de otro Application Load Balancer en la misma VPC. Si el otro Equilibrador de carga de aplicación está en una VPC que está interconectada a la VPC del equilibrador de carga, puede registrar sus direcciones IP.

IPv6 objetivos

- Las direcciones IP que registre deben estar dentro del bloque de CIDR de VPC o dentro de un bloque de CIDR de VPC emparejado.

Para registrar un destino o anular su registro mediante la dirección IP desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.

4. Elija la pestaña Destinos.
5. Para registrar direcciones IP, elija Registrar destinos. Para cada dirección IP, seleccione la red, introduzca la dirección IP y el puerto y elija Incluir como pendiente debajo.
6. Opcional: si la dirección IP está fuera de la VPC seleccionada, debe especificar una zona de disponibilidad.
7. Cuando haya terminado de especificar direcciones, elija Registrar destinos pendientes.
8. Para anular el registro de direcciones IP, selecciónelas y, a continuación, elija Anular registro. Si ha registrado muchas direcciones IP, puede que le resulte útil agregar un filtro o cambiar el orden.

## Registrar o anular el registro de una función de Lambda

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

Cómo registrar o anular el registro de una función de Lambda mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Si no hay ninguna función de Lambda registrada, elija Registrar. Seleccione la función de Lambda y elija Registrar.
6. Para anular el registro de una función de Lambda, elija Anular registro Cuando se le pida que confirme, elija Deregister.

## Registro o anulación del registro de destinos mediante la AWS CLI

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

# Uso de funciones de Lambda como destino de un Equilibrador de carga de aplicación

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

Límites

- La función de Lambda y el grupo de destino deben estar en la misma cuenta y en la misma región.
- El tamaño máximo del cuerpo de la solicitud que puede enviar a una función de 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 de Lambda puede enviar es de 1 MB.
- WebSockets no son compatibles. Las solicitudes de actualización se rechazan con el código HTTP 400.
- No se admiten las Zonas locales.
- No se admiten los pesos de destino automáticos (ATW).

Contenido



Para ver una demostración, consulte Destino de Lambda en Equilibrador de carga de aplicación.

## Preparar la función de Lambda

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

Permisos para invocar la función de Lambda

Si crea el grupo de destino y registra la función de Lambda utilizando la AWS Management Console, la consola añade los permisos necesarios a la política de su función de Lambda en su nombre. De lo contrario, después de crear el grupo objetivo y registrar la función mediante el AWS CLI, debe utilizar el comando add-permission para conceder a Elastic Load Balancing el permiso para invocar la función Lambda. Le recomendamos que use las claves de condición `aws:SourceAccount` y `aws:SourceArn` para restringir la invocación de la función al grupo de destino especificado. Para obtener más información, consulte El problema del suplente confuso en la Guía del usuario de IAM.

```
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 \
--source-account target-group-account-id
```

Control de versiones de funciones de Lambda

Puede registrar una sola función de Lambda por grupo de destino. Para asegurarse de que puede cambiar la función de Lambda y de que el equilibrador de carga siempre invoque la versión actual de la función de Lambda, cree un alias de función e incluya el alias en el ARN de la función cuando registre la función de Lambda en el equilibrador de carga. Para obtener más información, consulte los alias de las AWS Lambda funciones en la Guía para desarrolladores.AWS Lambda

Tiempo de espera de la función

El equilibrador de carga espera hasta que la función de Lambda responde o se agota el tiempo de espera. Le recomendamos que configure el tiempo de espera de la función de Lambda en función del tiempo de ejecución previsto. Para obtener información sobre el valor de tiempo de espera predeterminado y cómo cambiarlo, consulte Configurar el tiempo de espera de una función Lambda. Para obtener información sobre el valor de tiempo de espera máximo que puede configurar, consulte cuotas.AWS Lambda

## Creación de un grupo de destino para la función de Lambda

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

Cómo crear un grupo de destino y registrar la función de Lambda mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija Crear grupo de destino.
4. En Seleccionar un destino, elija Función de Lambda.
5. En Target group name, escriba el nombre del nuevo grupo de destino.
6. (Opcional) Para habilitar las comprobaciones, elija Comprobación de estado, Habilitar.
7. (Opcional) Agregue una o varias etiquetas, como se indica a continuación:
   a. Expanda la sección Etiquetas.
   b. Seleccione Agregar etiqueta.
   c. Escriba la clave y el valor de la etiqueta.
8. Elija Siguiente.
9. Especifique una sola función de Lambda u omita este paso y especifique una función de Lambda más adelante.
10. Elija Crear grupo de destino.

Cómo crear un grupo de destino y registrar la función de Lambda mediante la AWS CLI

Usa los comandos create-target-groupy register-targets.

## Recibir eventos del equilibrador de carga

El equilibrador de carga admite la invocación de Lambda de solicitudes a través de HTTP y HTTPS. El equilibrador de carga envía un evento en formato JSON. El equilibrador 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 encabezado `content-encoding` está presente, el equilibrador de carga Base64 codifica el cuerpo y establece `isBase64Encoded` en `true`.

Si el encabezado `content-encoding` no está presente, la codificación en Base64 depende del tipo de contenido. Para los siguientes tipos, el balanceador de cargas envía el cuerpo tal cual y lo establece `isBase64Encoded` en: text/*,. `false` application/json, application/javascript, and

application/xml Para todos los demás tipos, el equilibrador 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 equilibrador de carga

La respuesta de la función de Lambda debe incluir el estado de codificación en Base64, el código de estado y los encabezados. Puede omitir el cuerpo.

Para incluir contenido binario en el cuerpo de la respuesta, debe codificar en Base64 el contenido y establecer `isBase64Encoded` en `true`. El equilibrador 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 cargas no respeta los hop-by-hop encabezados, como o. `Connection` `Transfer-Encoding` Puede omitir el encabezado `Content-Length` porque el equilibrador de carga lo procesa antes de enviar las respuestas a los clientes.

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

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

Para ver las plantillas de funciones Lambda que funcionan con los balanceadores de carga de aplicaciones, consulta application-load-balancer-serverless-app en github. También puede abrir la consola de Lambda, elegir Aplicaciones, Crear una aplicación y seleccionar una de las siguientes opciones de entre AWS Serverless Application Repository:

- ALB-Lambda-Target- S3 UploadFileto
- ALB-Lambda-objetivo- BinaryResponse
- ALB-Lambda-Target- IP WhatisMy

## Encabezados de varios valores

Si las solicitudes de un cliente o las respuestas de una función de Lambda incluyen encabezados con varios valores o el mismo encabezado varias veces, o parámetros de consulta con varios valores para la misma clave, puede habilitar la compatibilidad con la sintaxis de encabezados de varios valores. Después de habilitar encabezados de varios valores, los encabezados y los parámetros de consulta intercambiados entre el equilibrador de carga y la función de Lambda utilizan matrices en lugar de cadenas. Si no habilita la sintaxis de encabezado de varios valores y un parámetro de encabezado o consulta tiene varios valores, el equilibrador de carga utiliza el último valor que reciba.

Contenido

- Respuestas con encabezados de varios valores
- Habilitar encabezados de varios valores

## 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 equilibrador 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 equilibrador 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 equilibrador 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 equilibrador 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"],
    ...
},
```

Si los parámetros de consulta están codificados en URL, el equilibrador de carga no los decodifica. Debe decodificarlos en la función de Lambda.

## 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, debe 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"]
  },
}
```

Es posible que el equilibrador de carga envíe los encabezados al cliente en un orden diferente al especificado en la carga útil de respuesta de Lambda. Por lo tanto, no espere que los encabezados se devuelvan en un orden específico.

### 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. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. Seleccione o desactive los encabezados con varios valores.
6. Seleccione Save changes (Guardar cambios).

Para habilitar los encabezados con varios valores, utilice el 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 de DNS con Amazon Route 53. La función de 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 de 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 de Lambda.

A continuación, se muestra el formato del evento de comprobación de estado enviado a la función de 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
}
```

Habilitación de las comprobaciones de estado de un grupo de destino mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Configuración de comprobación de estado, seleccione Editar.
5. En Comprobación de estado, seleccione Habilitar.
6. Seleccione Save changes (Guardar cambios).

Para habilitar los controles de estado de un grupo objetivo mediante el AWS CLI

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

## Anulación del registro de la función de Lambda

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

Para sustituir una función de 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 oyente para que utilicen el nuevo grupo de destino en lugar del existente.

Anulación del registro de la función de Lambda mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Destinos, elija Anular registro.
5. Cuando se le pida que confirme, elija Deregister.

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

Use el comando deregister-targets.

# Etiquetas para el grupo de destino del Equilibrador de carga de aplicación

Las etiquetas lo 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 eliminarla.

Restricciones

- Número máximo 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 iniciales ni finales.
- No utilice el `aws:` prefijo en los nombres o valores de las etiquetas, ya que está reservado para su uso. AWS Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar ni eliminar. 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. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar su página de detalles.
4. En la pestaña Etiquetas, elija Administrar etiquetas y realice una o varias de las acciones siguientes:
   a. Para actualizar una etiqueta, ingrese valores nuevos para Clave y Valor.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.
5. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de un grupo objetivo mediante el AWS CLI

Utilice los comandos add-tags y remove-tags.

# Eliminación de un grupo de destino del Equilibrador de carga de aplicación

Puede eliminar un grupo de destino si las acciones de las reglas de oyente no hacen referencia a él. La eliminación de un grupo de destino no afecta a los destinos registrados en él. Si ya no necesita una EC2 instancia registrada, puede detenerla o cancelarla.

Para eliminar un grupo de destino desde la consola

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

2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino y elija Actions, Delete.
4. Cuando se le indique que confirme, seleccione Sí, borrar.

Para eliminar un grupo objetivo mediante el AWS CLI

Utilice el comando delete-target-group.

# Monitorización de los equilibradores de carga de aplicaciones

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

CloudWatch métricas

Puedes usar Amazon CloudWatch para recuperar estadísticas sobre puntos de datos para tus balanceadores de carga y objetivos como un conjunto ordenado de datos de series temporales, conocidos como métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte CloudWatch métricas para su Application Load Balancer.

Registros de acceso

Puede utilizar los registros de acceso para capturar información detallada sobre las solicitudes realizadas al equilibrador de carga y almacenarla en archivos de registro en Amazon S3. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar problemas en los destinos. Para obtener más información, consulte Registros de acceso del Equilibrador de carga de aplicación.

Registros de conexiones

Puede utilizar los registros de conexión para capturar atributos sobre las solicitudes realizadas al equilibrador de carga y almacenarlos en archivos de registro en Amazon S3. Puede usar estos registros de conexión para determinar la dirección IP y el puerto del cliente, la información del certificado del cliente, los resultados de la conexión y los cifrados TLS que se utilizan. Estos registros de conexión se pueden usar luego para revisar los patrones de solicitudes y otras tendencias. Para obtener más información, consulte Registros de conexión del Equilibrador de carga de aplicación.

Rastreo de solicitudes

Puede utilizar el rastreo de solicitudes para realizar un seguimiento de las solicitudes HTTP. El equilibrador de carga agrega un encabezado con un identificador de rastreo a cada solicitud que recibe. Para obtener más información, consulte Solicite un rastreo de equilibrador de carga de aplicaciones..

CloudTrail registros

Se puede utilizar AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a la API de Elastic Load Balancing y almacenarlas como archivos de registro en Amazon S3. Puede usar estos CloudTrail registros para determinar qué llamadas se realizaron, la dirección IP de origen de la llamada, quién realizó la llamada, cuándo se realizó la llamada, etc. Para obtener más información, consulte Registrar llamadas a la API para Elastic Load Balancing mediante CloudTrail.

# CloudWatch métricas para su Application Load Balancer

Elastic Load Balancing publica puntos de datos en Amazon CloudWatch para sus balanceadores de carga y sus objetivos. CloudWatchle permite recuperar estadísticas sobre esos puntos de datos como un conjunto ordenado de datos de series temporales, conocidos como 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 equilibrador 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 CloudWatch alarma para supervisar una métrica específica e iniciar una acción (como enviar una notificación a una dirección de correo electrónico) si la métrica se encuentra fuera de lo que considera un rango aceptable.

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

Las métricas de los balanceadores de carga de aplicaciones excluyen las solicitudes de verificación de estado.

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

Contenido

- Estadísticas para métricas del Equilibrador de carga de aplicación
- Consulta CloudWatch las métricas de tu balanceador de cargas

## Métricas del Equilibrador de carga de aplicación

- Equilibradores de carga
- Destinos
- Estado del grupo de destino
- Funciones de Lambda
- Autenticación del usuario

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

| Métrica | Descripción |
| --- | --- |
| `ActiveConnectionCount` | El número total de conexiones TCP simultáneas activas desde los clientes al equilibrador de carga y desde el equilibrador de carga a los destinos.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |
| `AnomalousHostCount` | La cantidad de hosts detectados con anomalías.<br><br>Criterios del informe: se informa siempre<br><br>Estadísticas: las estadísticas más útiles son `Average`, `Minimum` y `Maximum`. |

| Métrica | Descripción |
| --- | --- |
| | Dimensiones<br>• `TargetGroup` , `LoadBalancer`<br>• `TargetGroup` , `AvailabilityZone` , `LoadBalancer` |
| `BYoIPUtilPercentage` | El porcentaje de uso del grupo de direcciones IP.<br>Criterios de presentación de informes: la BYo IP está habilitada en el balanceador de cargas.<br>Estadísticas: la única estadística relevante es `Average`.<br>Dimensiones<br>• `LoadBalancer` , `TargetGroup`<br>• `LoadBalancer` , `TargetGroup` , `AvailabilityZone` |
| `ClientTLSNegotiationErrorCount` | El número de conexiones TLS iniciadas por el cliente que no establecieron una sesión con el equilibrador de carga debido a un error de TLS. Las posibles causas incluyen la falta de coinciden cia de los cifrados o protocolos o que el cliente no pudo verificar el certificado del servidor y cerró la conexión.<br>Criterios del informe: hay un valor distinto de cero<br>Estadísticas: la estadística más útil es `Sum`.<br>Dimensiones<br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| `ConsumedLCUs` | El número de unidades de capacidad del equilibrador de carga (LCU) usadas por el equilibrador de carga. Pagas por la cantidad LCUs que utilices por hora. Cuando la reserva de la LCU esté activa, el LCUs consumidor informará `0` si el uso es inferior a la capacidad reservada e informará los valores superiores `0` si el uso supera la reservada LCUs. Para obtener más información, consulte Precios de Elastic Load Balancing.<br><br>Criterios del informe: se informa siempre<br><br>Estadísticas: todas<br><br>Dimensiones<br><br>• `LoadBalancer` |
| `PeakLCUs` | El número máximo de unidades de capacidad del balanceador de carga (LCU) utilizadas por el balanceador de carga en un momento dado. Solo se aplica cuando se utiliza LCU Reservation.<br><br>Criterios de presentación de informes: siempre<br><br>Estadísticas: las estadísticas más útiles son `Sum` y `Max`.<br><br>Dimensiones<br><br>• `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| `ReservedLCUs` | Una métrica de facturación que informa de la capacidad reservada por minuto. El importe total reservado LCUs durante cualquier período es el importe que se LCUs te cobrará. Por ejemplo, si LCUs se reservan 500 para una hora, la métrica por minuto será de LCUs 8,33. Para obtener más información, consulte Supervise la reserva.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: todas<br><br>Dimensiones<br><br>• `LoadBalancer` |
| `DesyncMitigationMode_NonCompliant_Request_Count` | El número de solicitudes que no cumplen con RFC 7230.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| `DroppedInvalidHeaderRequestCount` | Número de solicitudes en las que el equilibrador de carga eliminó encabezados HTTP con campos de encabezado que no son válidos antes de enrutar la solicitud. El equilibrador de carga quita estos encabezados solo si el atributo `routing.http.drop_invalid_header_fields.enabled` está establecido en `true`.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: todas<br><br>Dimensiones<br><br>• `AvailabilityZone` , `LoadBalancer` |
| `MitigatedHostCount` | El número de destinos que se están mitigando.<br><br>Criterios del informe: se informa siempre<br><br>Estadísticas: las estadísticas más útiles son `Average`, `Minimum` y `Maximum`.<br><br>Dimensiones<br><br>• `TargetGroup` , `LoadBalancer`<br>• `TargetGroup` , `AvailabilityZone` , `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| ForwardedInvalidHeaderRequestCount | Número de solicitudes enrutadas por el equilibrador de carga que tenían encabezados HTTP con campos de encabezado que no son válidos. El equilibrador de carga reenvía las solicitudes con estos encabezados solo si el atributo routing.http.drop_invalid_header_fields.enabled está establecido en false.<br><br>Criterios del informe: se informa siempre<br><br>Estadísticas: todas<br><br>Dimensiones<br><br>• AvailabilityZone , LoadBalancer |
| GrpcRequestCount | El número de solicitudes de gRPC procesadas durante IPv4 y. IPv6<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil esSum. Minimum, Maximum y Average todas devuelven 1.<br><br>Dimensiones<br><br>• LoadBalancer , TargetGroup<br>• AvailabilityZone , LoadBalancer , TargetGroup<br>• TargetGroup<br>• AvailabilityZone , TargetGroup |

| Métrica | Descripción |
| --- | --- |
| HTTP_Fixed_Response_Count | El número de acciones de respuesta fija que se han realizado correctamente.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| HTTP_Redirect_Count | El número de acciones de redireccionamiento que se han realizado correctamente.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , 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.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |

| Métrica | Descripción |
| --- | --- |
| HTTPCode_ELB_3XX_Count | El número de códigos de redireccionamiento de HTTP 3XX que proceden del equilibrador de carga. Este recuento no incluye los códigos de respuesta generados por los destinos.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| HTTPCode_ELB_4XX_Count | El número de códigos de error del cliente HTTP 4XX que proceden del equilibrador de carga. Este recuento no incluye los códigos de respuesta generados por los destinos.<br><br>Los errores del cliente se generan cuando las solicitudes no tienen el formato correcto o están incompletas. El destino no recibió estas solicitudes, excepto en el caso en que el equilibrador de carga devuelve un código de error HTTP 460. Este número no incluye los códigos de respuesta generados por los destinos.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil esSum. Minimum, Maximum y Average todas devuelven 1.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |

| Métrica | Descripción |
| --- | --- |
| HTTPCode_ELB_5XX_Count | El número de códigos de error del servidor HTTP 5XX que proceden del equilibrador de carga. Este número no incluye los códigos de respuesta generados por los destinos.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es `Sum`. `Minimum`, `Maximum` y `Average` todas devuelven 1.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |
| HTTPCode_ELB_500_Count | El número de códigos de error del servidor HTTP 500 que proceden del equilibrador de carga.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |
| HTTPCode_ELB_502_Count | El número de códigos de error del servidor HTTP 502 que proceden del equilibrador de carga.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| HTTPCode_ELB_503_Count | El número de códigos de error del servidor HTTP 503 que proceden del equilibrador de carga.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| HTTPCode_ELB_504_Count | El número de códigos de error del servidor HTTP 504 que proceden del equilibrador de carga.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| IPv6ProcessedBytes | El número total de bytes procesados por el balanceador de cargas es superior. IPv6 Este recuento se incluye en ProcessedBytes .<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |

| Métrica | Descripción |
| --- | --- |
| IPv6RequestCount | El número de IPv6 solicitudes recibidas por el balanceador de cargas.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil esSum. Minimum, Maximum y Average todas devuelven 1.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| NewConnectionCount | El número total de conexiones TCP nuevas establecidas desde los clientes al equilibrador de carga y desde el equilibrador de carga a los destinos.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |

| Métrica | Descripción |
| --- | --- |
| NonStickyRequestCount | El número de solicitudes para las que equilibrador de carga eligió un nuevo destino porque no pudo utilizar una sesión persistente 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 equilibrador de carga leyese la cookie de persistencia.<br><br>Reporting criteria (Criterios del informe): la persistencia está habilitada en el grupo de destino.<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| ProcessedBytes | El número total de bytes procesados por el balanceador de cargas a través de IPv4 y IPv6 (encabezado HTTP y carga útil HTTP). Este recuento incluye el tráfico entrante y saliente de los clientes y las funciones de Lambda, así como el tráfico de un proveedor de identidades (IdP) si la autenticación de usuarios está habilitada.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |

| Métrica | Descripción |
| --- | --- |
| RejectedConnectionCount | El número de conexiones que se rechazaron porque el equilibrador de carga alcanzó el número máximo de conexiones.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| RequestCount | El número de solicitudes procesadas durante IPv4 y. IPv6 Esta métrica solo se incrementa para las solicitudes en las que el nodo del equilibrador de carga pudo elegir un destino. Las solicitudes que se rechazan antes de elegir un destino no se reflejan en esta métrica.<br><br>Criterios de notificación: se notifica si hay destinos registrados.<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• LoadBalancer , AvailabilityZone<br>• LoadBalancer , TargetGroup<br>• LoadBalancer , AvailabilityZone , TargetGroup |

| Métrica | Descripción |
| --- | --- |
| RuleEvaluations | El número de reglas que evalúa el equilibrador de carga al procesar las solicitudes. La regla predeterminada no se cuenta. En este recuento se incluyen las 10 evaluaciones de reglas gratuitas por solicitud.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer |
| ZonalShiftedHostCount | El número de objetivos que se consideran inhabilitados debido al cambio zonal.<br><br>Criterios de presentación de informes: se informa cuando hay un valor<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer , TargetGroup .<br>• AvailabilityZone , LoadBalancer , TargetGroup . |

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.<br><br>Criterios de notificación: se notifica si hay destinos registrados.<br><br>Estadísticas: las estadísticas más útiles son Average, Minimum y Maximum. |

| Métrica | Descripción |
| --- | --- |
| | Dimensiones<br>• `LoadBalancer` , `TargetGroup`<br>• `LoadBalancer` , `AvailabilityZone` , `TargetGroup` |
| `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 equilibrador de carga.<br>Criterios de notificación: se notifica si hay destinos registrados.<br>Estadísticas: la estadística más útil es`Sum`. `Minimum`, `Maximum` y `Average` todas devuelven 1.<br>Dimensiones<br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer`<br>• `TargetGroup` , `LoadBalancer`<br>• `TargetGroup` , `AvailabilityZone` , `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| `RequestCountPerTarget` | El recuento medio de solicitudes por destino, en 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 de Lambda.<br><br>Este recuento utiliza el número total de solicitudes que recibe el grupo de destino, y lo divide por el número de destinos en buen estado del grupo. Si no hay destinos en buen estado en el grupo de destino, se divide entre el número total de destinos registrados.<br><br>Criterios del informe: se informa siempre<br><br>Estadísticas: la única estadística válida es `Sum`. Esto representa la media, no la suma.<br><br>Dimensiones<br><br>• `TargetGroup`<br>• `TargetGroup` , `AvailabilityZone`<br>• `LoadBalancer` , `TargetGroup`<br>• `LoadBalancer` , `AvailabilityZone` , `TargetGroup` |

| Métrica | Descripción |
| --- | --- |
| TargetConnectionErrorCount | El número de conexiones que no se establecieron correctamente entre el equilibrador de carga y el destino. Esta métrica no se aplica si el destino es una función de Lambda. Esta métrica no se increment a si las conexiones de comprobación de estado no son correctas.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer<br>• TargetGroup , LoadBalancer<br>• TargetGroup , AvailabilityZone , LoadBalancer |
| TargetResponseTime | El tiempo transcurrido, en segundos, desde que la solicitud abandona el equilibrador de carga hasta que el destino comienza a enviar los encabezados de la respuesta. Esto equivale al campo target_processing_time de los registros de acceso.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: las estadísticas más útiles son Average y pNN.NN (percentiles).<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer<br>• TargetGroup , LoadBalancer<br>• TargetGroup , AvailabilityZone , LoadBalancer |

| Métrica | Descripción |
| --- | --- |
| TargetTLSNegotiationErrorCount | El número de conexiones TLS iniciadas por el equilibrador 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 de Lambda.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer<br>• TargetGroup , LoadBalancer<br>• TargetGroup , AvailabilityZone , LoadBalancer |
| UnHealthyHostCount | El número de destinos que se considera que no están en buen estado.<br><br>Al anular el registro de un objetivo, este porcentaje disminuye HealthyHostCount pero no aumenta. UnhealthyHostCount<br><br>Criterios de notificación: se notifica si hay destinos registrados.<br><br>Estadísticas: las estadísticas más útiles son Average, Minimum y Maximum.<br><br>Dimensiones<br><br>• LoadBalancer , TargetGroup<br>• LoadBalancer , AvailabilityZone , TargetGroup |

El espacio de nombres AWS/ApplicationELB incluye las siguientes métricas para el estado del grupo de destino. Para obtener más información, consulte the section called “Estado del grupo de destino”.

| Métrica | Descripción |
| --- | --- |
| HealthyStateDNS | La cantidad de zonas que cumplen los requisitos de estado correcto del DNS.<br><br>Estadísticas: la estadística más útil es Max.<br><br>Dimensiones<br><br>• LoadBalancer , TargetGroup<br>• AvailabilityZone , LoadBalancer , TargetGroup |
| HealthyStateRouting | La cantidad de zonas que cumplen los requisitos de estado correcto del enrutamiento.<br><br>Estadísticas: la estadística más útil es Max.<br><br>Dimensiones<br><br>• LoadBalancer , TargetGroup<br>• AvailabilityZone , LoadBalancer , TargetGroup |
| UnhealthyRoutingRequestCount | La cantidad de solicitudes que se enrutan mediante la acción de conmutación por error de enrutamiento (apertura por error).<br><br>Estadísticas: la estadística más útil es Sum.<br><br>Dimensiones<br><br>• LoadBalancer , TargetGroup<br>• AvailabilityZone , LoadBalancer , TargetGroup |
| UnhealthyStateDNS | La cantidad de zonas que no cumplen los requisitos de estado correcto del DNS y, por lo tanto, se marcaron como zonas en mal estado en el DNS.<br><br>Estadísticas: la estadística más útil es Min. |

| Métrica | Descripción |
| --- | --- |
| | Dimensiones<br>• `LoadBalancer` , `TargetGroup`<br>• `AvailabilityZone` , `LoadBalancer` , `TargetGroup` |
| `UnhealthyStateRouting` | La cantidad de zonas que no cumplen los requisitos de estado correcto del enrutamiento y, por lo tanto, el equilibrador de carga distribuye el tráfico a todos los destinos de la zona, incluidos los destinos en mal estado.<br>Estadísticas: la estadística más útil es `Min`.<br>Dimensiones<br>• `LoadBalancer` , `TargetGroup`<br>• `AvailabilityZone` , `LoadBalancer` , `TargetGroup` |

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

| Métrica | Descripción |
| --- | --- |
| `LambdaInternalError` | El número de solicitudes dirigidas a una función de Lambda que produjeron un error debido a un problema con el equilibrador de carga o AWS Lambda. Para obtener los códigos de los motivos de error, consulte el campo error_reason del registro de acceso.<br>Criterios del informe: hay un valor distinto de cero<br>Estadísticas: la única estadística relevante es `Sum`.<br>Dimensiones<br>• `TargetGroup`<br>• `TargetGroup` , `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| LambdaTargetProcessedBytes | El número total de bytes procesados por el equilibrador de carga para las solicitudes y las respuestas de una función de Lambda.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer |
| LambdaUserError | El número de solicitudes dirigidas a una función de Lambda que produjeron un error debido a un problema con la función de Lambda. Por ejemplo, el equilibrador de carga no tenía permiso para invocar la función, el equilibrador 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.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• TargetGroup<br>• TargetGroup , LoadBalancer |

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 |

| Métrica | Descripción |
| --- | --- |
| | acción de autenticación o el equilibrador 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.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `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.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |

| Métrica | Descripción |
| --- | --- |
| 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.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: todas las estadísticas son relevantes.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |
| ELBAuthRefreshTokenSuccess | El número de veces que el equilibrador de carga actualizó correctamente las notificaciones de usuario con un token de actualización proporcionado por el proveedor de identidad.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es Sum.<br><br>Dimensiones<br><br>• LoadBalancer<br>• AvailabilityZone , LoadBalancer |

| Métrica | Descripción |
| --- | --- |
| `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 equilibrador de carga haya recuperado las notificaciones de usuario del IdP.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la estadística más útil es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |
| `ELBAuthUserClaimsSizeExceeded` | El número de veces que un proveedor de identidad devolvió las notificaciones de usuario con un tamaño superior a 11 K.<br><br>Criterios del informe: hay un valor distinto de cero<br><br>Estadísticas: la única estadística relevante es `Sum`.<br><br>Dimensiones<br><br>• `LoadBalancer`<br>• `AvailabilityZone` , `LoadBalancer` |

## Dimensiones de las métricas de los equilibradores de carga de aplicaciones

Para filtrar las métricas del Equilibrador de carga de aplicación, use las siguientes dimensiones.

| Dimensión | Descripción |
| --- | --- |
| `AvailabilityZone` | Filtra los datos de métricas por zona de disponibilidad. |

| Dimensión | Descripción |
| --- | --- |
| `LoadBalancer` | Filtra los datos de métricas por equilibrador de carga. Especifique el balanceador de carga de la siguiente manera: app/ load-balancer-name /1234567890123456 (la parte final del ARN del balanceador de carga). |
| `TargetGroup` | Filtra los datos de métricas por grupo de destino. Especifique el grupo objetivo de la siguiente manera: target-group-nametargetgroup/ 1234567890123456 (la parte final del ARN del grupo objetivo). |

## Estadísticas para métricas del Equilibrador de carga de aplicación

CloudWatch proporciona estadísticas basadas en los puntos de datos métricos publicados 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 de todas las EC2 instancias en buen estado de un balanceador de carga lanzado en una zona de disponibilidad específica.

Las estadísticas `Minimum` y `Maximum` reflejan los valores mínimo y máximo de los puntos de datos registrados en los nodos individuales del equilibrador de carga en cada ventana de muestreo. Por ejemplo, supongamos que hay 2 nodos de equilibrador de carga que componen el Equilibrador de carga de aplicación. 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 equilibrador de carga en su conjunto, `Minimum` es 1, `Maximum` es 10 y `Average` es aproximadamente 4.

Le recomendamos que controle los `UnHealthyHostCount` distintos de cero en la estadística de `Minimum` y que active la alarma si los valores son distintos de cero en más de un punto de datos. El uso de `Minimum` detectará si cada nodo y zona de disponibilidad del equilibrador de carga considera que los destinos no tienen el estado correcto. La alarma activada en `Average` o `Maximum` es útil si quiere recibir alertas sobre posibles problemas, por lo que recomendamos a los clientes que revisen esta métrica e investiguen los casos en los que los valores sean distintos a cero. La mitigación automática de los errores se puede realizar siguiendo las prácticas recomendadas de utilizar la comprobación del estado del balanceador de carga en Amazon EC2 Auto Scaling o Amazon Elastic Container Service (Amazon ECS).

La estadística `Sum` es el valor de la suma para todos los nodos del equilibrador 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 equilibrador 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 equilibrador 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 rendimiento de la aplicación. Al usar el percentil 99 como disparador o CloudWatch alarma de Auto Scaling, puede tener como objetivo que no más del 1 por ciento de las solicitudes tarden más de 2 ms en procesarse.

## Consulta CloudWatch las métricas de tu balanceador de cargas

Puedes ver las CloudWatch métricas de tus balanceadores de carga mediante la EC2 consola de Amazon. Estas métricas se muestran en gráficos de monitorización. Los gráficos de monitorización muestran puntos de datos si el equilibrador 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

1. Abre la EC2 consola de Amazon 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 equilibrador de carga, haga lo siguiente:

   a. En el panel de navegación, seleccione Equilibradores de carga.
   b. Seleccione el equilibrador de carga y, a continuación, elija la pestaña Monitorizar.
   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 ver las métricas mediante la CloudWatch consola

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione ApplicationELB espacio de nombre.
4. (Opcional) Para ver una métrica en todas las dimensiones, ingrese 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 equilibradores de carga, elija Por métrica de AppELB. Para ver las métricas de un solo equilibrador de carga, escriba su nombre en el campo de búsqueda.
   - Para mostrar solamente las métricas registradas para los grupos de destino, elija Por métrica de AppELB, de TG. 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 equilibradores de carga por zona de disponibilidad, elija Por métrica de AppELB, de AZ. Para ver las métricas de un solo equilibrador 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 equilibradores de carga por zona de disponibilidad y el grupo de destino, elija Por métricas de AppELB, de AZ, de TG. Para ver las métricas de un solo equilibrador 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 las métricas mediante el 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 mediante el AWS CLI

Use el siguiente get-metric-statisticscomando para obtener estadísticas para la métrica y la dimensión especificadas. CloudWatch trata cada combinación única 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 de la salida:

```
{
    "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"
}
```

# Registros de acceso del Equilibrador de carga de aplicación

Elastic Load Balancing proporciona registros de acceso que capturan información detallada sobre las solicitudes enviadas al equilibrador de carga. Cada registro 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 registros de acceso para analizar los patrones de tráfico y solucionar problemas.

Los registros de acceso son una característica opcional de Elastic Load Balancing que está desactivada de forma predeterminada. Una vez que se han habilitado los registros de acceso del equilibrador de carga, Elastic Load Balancing captura los registros y los almacena en el bucket de Amazon S3 que haya especificado como archivos comprimidos. Puede deshabilitar los registros de acceso en cualquier momento.

Se cobran los costos de almacenamiento en Amazon S3, pero no el ancho de banda que Elastic Load Balancing utilice para enviar los archivos de registros a Amazon S3. Para obtener más información acerca de los costos de almacenamiento, consulte Precios de Amazon S3.

Contenido



## Archivos de registro de acceso

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

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

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

bucket

Nombre del bucket de S3.

prefix

(Opcional) El prefijo (jerarquía lógica) del bucket. El prefijo que especifique no debe incluir la cadena `AWSLogs`. Para obtener más información, consulte Organizar objetos con prefijos.

`AWSLogs`

Agregamos la parte del nombre de archivo que comienza por `AWSLogs` después del nombre del bucket y el prefijo que especifique.

aws-account-id

El ID de AWS cuenta del propietario.

region

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

aaaa/mm/dd

La fecha de entrega del registro.

load-balancer-id

ID de recurso del equilibrador 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 en la zona horaria de Zulu o UTC.

ip-address

La dirección IP del nodo del equilibrador de carga que controló la solicitud. Si se trata de un equilibrador 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 archivo de registro con el prefijo:

```
s3://amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/
elasticloadbalancing/us-east-2/2022/05/01/123456789012_elasticloadbalancing_us-
```

```
east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

A continuación, se muestra un ejemplo de nombre de archivo de registro sin un prefijo:

```
s3://amzn-s3-demo-logging-bucket/AWSLogs/123456789012/elasticloadbalancing/
us-east-2/2022/05/01/123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

Puede almacenar los archivos de registro en su 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 Gestión del ciclo de vida de los objetos en la Guía del usuario de Amazon S3.

## Entradas de los registros de acceso

Elastic Load Balancing registra las solicitudes enviadas al equilibrador de carga, incluidas las que nunca 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. Elastic Load Balancing no registra las solicitudes de comprobación de estado.

Cada entrada de registro contiene los detalles de una sola solicitud (o conexión, en su caso WebSockets) realizada al balanceador de cargas. WebSocketsEn efecto, una entrada se escribe solo después de cerrar 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 registros de acceso para comprender la naturaleza de las solicitudes y no como una relación exhaustiva de todas las solicitudes.

Contenido

- Códigos de motivo de error

## Sintaxis

En la siguiente tabla se describen los campos de una entrada de registro 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):<br>• `http` — HTTP<br>• `https` — HTTP sobre TLS<br>• `h2` — HTTP/2 sobre SSL/TLS<br>• `grpcs` — gRPC sobre TLS<br>• `ws` — WebSockets<br>• `wss`— a WebSockets través de TLS |
| time | Hora a la que el equilibrador de carga generó una respuesta al cliente, en formato ISO 8601. Pues WebSockets, este es el momento en que se cierra la conexión. |
| elb | ID de recurso del equilibrador de carga. Si está analizando las entradas del registro de acceso, tenga en cuenta que los recursos IDs pueden contener barras diagonales (/). |
| client:port | Dirección IP y puerto del cliente solicitante. Si hay un proxy delante del equilibrador de carga, este campo contiene la dirección IP del proxy. |
| target:port | Dirección IP y puerto del destino que procesó esta solicitud.<br>Si el cliente no envió una solicitud completa, el equilibrador de carga no puede enviar la solicitud a un destino, en cuyo caso este valor se establece en -. |

| Campo | Descripción |
| --- | --- |
| | Si el destino es una función de Lambda, este valor se establece en -.<br><br>Si la solicitud está bloqueada por AWS WAF, este valor se establece en -. |
| request_processing_time | Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el equilibrador de carga recibió la solicitud hasta que se la envió a un destino.<br><br>Este valor también se establece en -1 si el equilibrador 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.<br><br>Este valor también se puede establecer en -1 si no es posible establecer una conexión TCP con el destino antes de que se agote el tiempo de espera de 10 segundos de la conexión TCP.<br><br>Si AWS WAF está habilitada para su Application Load Balancer o el tipo de destino es una función Lambda, se tendrá en cuenta el tiempo que tarda el cliente en enviar los datos necesarios para las solicitudes POST. `request_processing_time` |

| Campo | Descripción |
| --- | --- |
| target_processing_time | Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el equilibrador de carga envió la solicitud a un destino hasta que este comenzó a enviar los encabezados de la respuesta.<br><br>Este valor también se establece en -1 si el equilibrador 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.<br><br>Este valor también se puede establecer en -1 si el destino registrado no responde antes de que se agote el tiempo de inactividad.<br><br>Si no AWS WAF está activado para su Application Load Balancer, se tendrá en cuenta el tiempo que tarda el cliente en enviar los datos necesarios para las solicitudes POST. `target_processing_time` |
| response_processing_time | Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el equilibrador 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 equilibrador de carga como tiempo de adquisición de la conexión entre el equilibrador de carga y el cliente.<br><br>Este valor se establece en -1 si el equilibrador de carga no recibe una respuesta de 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 | El código de estado de la respuesta generado por el balanceador de cargas, la regla de respuesta fija o el código de respuesta AWS WAF personalizado para las acciones de bloqueo. |
| 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 -. |

| Campo | Descripción |
| --- | --- |
| received_bytes | Tamaño de la solicitud, en bytes, recibida desde el cliente (solicitante). Para las solicitudes HTTP, incluye los encabezados. Pues WebSockets, este es el número total de bytes recibidos del cliente en la conexión. |
| sent_bytes | Tamaño de la respuesta, en bytes, enviada al cliente (solicitante). En el caso de las solicitudes HTTP, esto incluye los encabezados y el cuerpo de la respuesta. Pues WebSockets, este es el número total de bytes enviados al cliente en la conexión.<br><br>Los encabezados TCP y la carga útil del protocolo de enlace TLS no se cuentan y no tienen correlación con la entrada. `DataTransfer-Out-Bytes` AWS Cost Explorer |
| “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 equilibrador 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 oyente no es un oyente HTTPS. |
| ssl_protocol | [Agente de escucha HTTPS] El protocolo SSL. Este valor se establece en - si el oyente no es un oyente 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. |

| Campo | Descripción |
| --- | --- |
| “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. Este valor se establece en - si el oyente no es un oyente HTTPS. |
| 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 equilibrador 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 valores que se describen en Medidas tomadas. 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. Si las acciones realizadas no incluyen una acción de autenticación o el destino no es una función de Lambda, este valor se establece en -. |

| Campo | Descripción |
| --- | --- |
| “target:port_list” | Una lista delimitada por espacios de direcciones IP y puertos para los destinos que procesaron esta solicitud, entre comillas dobles. Actualmente, esta lista puede contener un elemento y coincide con el campo target:port.<br><br>Si el cliente no envió una solicitud completa, el equilibrador de carga no puede enviar la solicitud a un destino, en cuyo caso este valor se establece en -.<br><br>Si el destino es una función de Lambda, este valor se establece en -.<br><br>Si la solicitud está bloqueada por AWS WAF, este valor se establece en -. |
| “target_status_code_list” | Una lista delimitada por espacios de códigos de estado de las respuestas de los destinos, entre comillas dobles. Actualmente, esta lista puede contener un elemento y coincide con el campo target_status_code.<br><br>Este valor se registra únicamente si se estableció una conexión con el destino y este envió una respuesta. De lo contrario, se establece en -. |
| “classification” | La clasificación de la mitigación de la desincronización, entre comillas dobles. Si la solicitud no cumple con RFC 7230, los valores posibles son Aceptable, Ambiguo y Grave.<br><br>Si la solicitud cumple con RFC 7230, este valor se establece en -. |
| “classification_reason” | El código de motivo de la clasificación, entre comillas dobles. Si la solicitud no cumple con la RFC 7230, se trata de uno de los códigos de clasificación descritos en Motivos de la clasificación. Si la solicitud cumple con RFC 7230, este valor se establece en -. |

| Campo | Descripción |
| --- | --- |
| conn_trace_id | El identificador de trazabilidad de la conexión es un identificador opaco único que se utiliza para identificar cada conexión. Una vez estableci da una conexión con un cliente, las solicitudes posteriores del cliente incluirán este ID en sus respectivas entradas del registro de acceso. Este ID funciona como una clave externa para crear un enlace entre los registros de conexión y acceso. |

## Medidas tomadas

El equilibrador de carga almacena las acciones que realiza en el campo actions_executed del registro de acceso.

- `authenticate`: el equilibrador de carga validó la sesión, autenticó al usuario y agregó la información del usuario a los encabezados de las solicitudes, según lo especificado en la configuración de la regla.
- `fixed-response`: el equilibrador de carga emitió una respuesta fija, según lo especificado en la configuración de la regla.
- `forward`: el equilibrador de carga reenvió la solicitud a un destino, según lo especificado en la configuración de la regla.
- `redirect`: el equilibrador de carga redirigió la solicitud a otra URL, según lo especificado en la configuración de la regla.
- `waf`: el equilibrador de carga reenvió la solicitud a AWS WAF para determinar si debía reenviarse al destino. Si esta es la acción final, AWS WAF determina que la solicitud debe rechazarse. De forma predeterminada, las solicitudes rechazadas por se AWS WAF registrarán como «403» en el `elb_status_code` campo. Si AWS WAF está configurado para rechazar solicitudes con un código de respuesta personalizado, el `elb_status_code` campo reflejará el código de respuesta configurado.
- `waf-failed`— El balanceador de cargas intentó reenviar la solicitud AWS WAF, pero el proceso falló.

## Motivos de la clasificación

Si una solicitud no cumple con RFC 7230, el equilibrador de carga almacena uno de los siguientes códigos en el campo classification_reason del registro de acceso. Para obtener más información, consulte Modo de mitigación de desincronización.

| Código | Descripción | Clasificación |
|---|---|---|
| `AmbiguousUri` | El URI de la solicitud contiene caracteres de control. | Ambigua |
| `BadContentLength` | El encabezado Content-Length contiene un valor que no se puede analizar o que no es un número válido. | Grave |
| `BadHeader` | Un encabezado contiene un carácter nulo o un retorno de carro. | Grave |
| `BadTransferEncoding` | El encabezado Transfer-Encoding contiene un valor incorrecto. | Grave |
| `BadUri` | El URI de la solicitud contiene un carácter nulo o un retorno de carro. | Grave |
| `BadMethod` | El método de la solicitud tiene un formato incorrecto. | Grave |
| `BadVersion` | La versión de la solicitud tiene un formato incorrecto. | Grave |
| `BothTeClPresent` | La solicitud contiene un encabezado Transfer-Encoding y un encabezado Content-Length. | Ambigua |
| `DuplicateContentLength` | Hay varios encabezados Content-Length con el mismo valor. | Ambigua |
| `EmptyHeader` | Un encabezado está vacío o hay una línea que solo contiene espacios. | Ambigua |

| Código | Descripción | Clasificación |
| --- | --- | --- |
| `GetHeadZeroContentLength` | Hay un encabezado Content-Length con un valor de 0 para una solicitud GET o HEAD. | Aceptable |
| `MultipleContentLength` | Hay varios encabezados Content-Length con valores diferentes. | Grave |
| `MultipleTransferEncodingChunked` | Hay varios encabezados Transfer-Encoding fragmentados. | Grave |
| `NonCompliantHeader` | Un encabezado contiene un carácter de control o no ASCII. | Aceptable |
| `NonCompliantVersion` | La versión de la solicitud contiene un valor incorrecto. | Aceptable |
| `SpaceInUri` | El URI de la solicitud contiene un espacio sin codificación URL. | Aceptable |
| `SuspiciousHeader` | Hay un encabezado que se puede normalizar a Transfer-Encoding o Content-Length mediante técnicas comunes de normalización de texto. | Ambigua |
| `SuspiciousTeClPresent` | La solicitud contiene un encabezado Transfer-Encoding y un encabezado Content-Length, y al menos uno de ellos es sospechoso. | Grave |
| `UndefinedContentLengthSemantics` | Hay un encabezado Content-Length definido para una solicitud GET o HEAD. | Ambigua |
| `UndefinedTransferEncodingSemantics` | Hay un encabezado Transfer-Encoding definido para una solicitud GET o HEAD. | Ambigua |

## Códigos de motivo de error

Si el equilibrador de carga no puede completar una acción de autenticación, el equilibrador de carga almacena uno de los siguientes códigos de motivo de error en el campo error_reason del registro de acceso. El balanceador de cargas también incrementa la métrica correspondiente. CloudWatch Para obtener más información, consulte Autenticación de usuarios mediante un Equilibrador de carga de aplicación.

| Código | Descripción | Métrica |
|---|---|---|
| `AuthInvalidCookie` | La cookie de autenticación no es válida. | `ELBAuthFailure` |
| `AuthInvalidGrantError` | El código de concesión de autorización del punto de conexión 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 conexión del token no es válida. | `ELBAuthFailure` |
| `AuthInvalidUserinfoResponse` | La respuesta desde el punto de conexión de información de usuario no es válida. | `ELBAuthFailure` |
| `AuthMissingCodeParam` | En la respuesta de autenticación desde el punto de conexión de autorización falta un parámetro de consulta denominado ‘code’. | `ELBAuthFailure` |
| `AuthMissingHostHeader` | En la respuesta de autenticación desde el punto de conexión de autorización falta un campo de encabezado de host. | `ELBAuthError` |

| Código | Descripción | Métrica |
| --- | --- | --- |
| `AuthMissingStateParam` | En la respuesta de autenticación desde el punto de conexión de autorización falta un parámetro de consulta denominado ‘state’. | `ELBAuthFailure` |
| `AuthTokenEpRequestFailed` | Hay una respuesta de error (no 2XX) del punto de conexión del token. | `ELBAuthError` |
| `AuthTokenEpRequestTimeout` | El balanceador de cargas no puede comunicarse con el punto final del token o el punto final del token no responde en 5 segundos. | `ELBAuthError` |
| `AuthUnhandledException` | El equilibrador de carga encontró una excepción no administrada. | `ELBAuthError` |
| `AuthUserinfoEpRequestFailed` | Hay una respuesta de error (no 2XX) del punto de conexión de información de usuario de IdP. | `ELBAuthError` |
| `AuthUserinfoEpRequestTimeout` | El balanceador de cargas no puede comunicarse con el punto final de información de usuario del IdP o el punto final de información de usuario no responde en 5 segundos. | `ELBAuthError` |
| `AuthUserinfoResponseSizeExceeded` | El tamaño de las reclamaciones devueltas por el IdP supera los 11K bytes. | `ELBAuthUserClaimsSizeExceeded` |

Si se produce un error en una solicitud a un grupo de destino ponderado, el equilibrador de carga almacena uno de los siguientes códigos de error en el campo error_reason del registro de acceso.

| Código | Descripción |
| --- | --- |
| `AWSALBTGCookieInvalid` | La AWSALBTG cookie, que se utiliza con los grupos objetivo ponderados, no es válida. Por ejemplo, el equilibrador de carga |

| Código | Descripción |
| --- | --- |
| | devuelve este error cuando los valores de la cookie están codificados como URL. |
| `WeightedTargetGroupsUnhandledException` | El equilibrador de carga encontró una excepción no administrada. |

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

| Código | Descripción | Métrica |
| --- | --- | --- |
| `LambdaAccessDenied` | El equilibrador de carga no tenía permiso para invocar la función de Lambda. | `LambdaUserError` |
| `LambdaBadRequest` | Se ha producido un error en la invocación lambda porque los encabezados o el cuerpo de la solicitud del cliente no contenían únicamente caracteres UTF-8. | `LambdaUserError` |
| `LambdaConnectionError` | El equilibrador de carga no puede conectarse a Lambda. | `LambdaInternalError` |
| `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 limitó Lambda durante la inicialización de la función. | `LambdaUserError` |

| Código | Descripción | Métrica |
| --- | --- | --- |
| `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 de Lambda porque se superó el límite de interfaces de red. | `LambdaUserError` |
| `LambdaInvalidResponse` | La respuesta de la función de Lambda no tiene el formato correcto o no incluye campos obligatorios. | `LambdaUserError` |
| `LambdaInvalidRuntimeException` | La versión especificada del tiempo de ejecución de Lambda no se admite. | `LambdaUserError` |
| `LambdaInvalidSecurityGroupIDException` | El ID de grupo de seguridad especificado en la configuración de la función de Lambda no es válido. | `LambdaUserError` |
| `LambdaInvalidSubnetIDException` | El ID de subred especificado en la configuración de la función de 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 de Lambda. | `LambdaUserError` |

| Código | Descripción | Métrica |
| --- | --- | --- |
| `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 de 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 de 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 de Lambda. | `LambdaUserError` |
| `LambdaRequestTooLarge` | El tamaño del cuerpo de la solicitud era superior a 1 MB. | `LambdaUserError` |
| `LambdaResourceNotFound` | No se pudo encontrar la función de 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 de Lambda porque una o varias subredes no tenían direcciones IP disponibles. | `LambdaUserError` |
| `LambdaThrottling` | La función de Lambda se rechazó porque había demasiadas solicitudes. | `LambdaUserError` |

| Código | Descripción | Métrica |
| --- | --- | --- |
| `LambdaUnhandled` | La función de Lambda encontró una excepción no administrada. | `LambdaUserError` |
| `LambdaUnhandledException` | El equilibrador de carga encontró una excepción no administrada. | `LambdaInternalError` |
| `LambdaWebsocketNotSupported` | WebSockets Lambda no los admite. | `LambdaUserError` |

Si el balanceador de cargas detecta un error al reenviar las solicitudes AWS WAF, almacena uno de los siguientes códigos de error en el campo error_reason del registro de acceso.

| Código | Descripción |
| --- | --- |
| `WAFConnectionError` | El balanceador de cargas no se puede conectar a. AWS WAF |
| `WAFConnectionTimeout` | Se agotó el AWS WAF tiempo de espera de la conexión. |
| `WAFResponseReadTimeout` | Se ha agotado el AWS WAF tiempo de espera de una solicitud. |
| `WAFServiceError` | AWS WAF devolvió un error de 5XX. |
| `WAFUnhandledException` | El equilibrador de carga encontró una excepción no administrada. |

## Ejemplo de entradas de registro

A continuación, se muestran ejemplos de entradas de registro. Tenga en cuenta que el texto del ejemplo aparece en varias líneas solo para facilitar su lectura.

Ejemplo de entrada HTTP

A continuación se muestra un ejemplo de entrada de registro para un oyente 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" "-" "-" "10.0.0.1:80" "200" "-" "-"
 TID_1234abcd5678ef90
```

Ejemplo de entrada HTTPS

A continuación se muestra un ejemplo de entrada de registro para un oyente 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" "-" "-" "10.0.0.1:80" "200" "-"
 "-" TID_1234abcd5678ef90
```

Ejemplo de entrada HTTP/2

A continuación se muestra un ejemplo de entrada de registro 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/" "-" "10.0.0.66:9000"
 "200" "-" "-" TID_1234abcd5678ef90
```

Ejemplo de WebSockets entrada

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

```
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" "-" "-" "10.0.1.192:8010" "101" "-" "-"
 TID_1234abcd5678ef90
```

Ejemplo de WebSockets entrada segura

A continuación se muestra un ejemplo de entrada de registro para una WebSockets conexión 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" "-" "-" "10.0.0.171:8010" "101" "-" "-"
 TID_1234abcd5678ef90
```

Entradas de ejemplo de funciones de Lambda

A continuación, se muestra una entrada de registro de ejemplo de una solicitud dirigida a una función de 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" "-" "-" "-" "-" "-" "-" TID_1234abcd5678ef90
```

A continuación, se muestra una entrada de registro de ejemplo de una solicitud dirigida a una función de 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" "-" "-" "-" "-"
 TID_1234abcd5678ef90
```

## Procesamiento de archivos de registro de acceso

Los archivos de registro de acceso están comprimidos. Si descarga los archivos, debe descomprimirlos para ver la información.

Si existe una gran cantidad de demanda en el sitio web, el equilibrador de carga puede generar archivos registro con gigabytes de datos. Es posible que no pueda procesar una cantidad tan grande de datos mediante el line-by-line procesamiento. 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 registros 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, revise Consulta de registros del Equilibrador de carga de aplicación en la Guía del usuario de Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

## Registros de acceso del Equilibrador de carga de aplicación

Al habilitar los registros de acceso del equilibrador de carga, debe especificar el nombre del bucket de S3 donde el equilibrador de carga almacenará los registros. El bucket debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir en el bucket.

Tareas

- Paso 1: Crear un bucket de S3
- Paso 2: Adjuntar una política al bucket de S3
- Paso 3: configurar los registros de acceso

- Paso 4: verificar los permisos del bucket
- Solución de problemas

## Paso 1: Crear un bucket de S3

Al habilitar los registros de acceso, es preciso especificar un bucket de S3 para estos. Puede utilizar un bucket existente o crear uno específico para los registros de acceso. El bucket debe cumplir los siguientes requisitos.

Requisitos

- El bucket debe estar ubicado en la misma región que el equilibrador de carga. El bucket y el equilibrador de carga pueden ser propiedad de diferentes cuentas.
- La única opción de cifrado del lado del servidor que se admite son claves administradas por Amazon S3 (SSE-S3). Para obtener más información, consulte Claves de cifrado administradas por Amazon S3 (SSE-S3).

Para crear un bucket de S3 con la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Elija Crear bucket.
3. En la página Crear un bucket, realice las siguientes acciones:
   a. En Nombre del bucket, escriba un nombre para el bucket. Este nombre debe ser único entre todos los nombres de buckets de Amazon S3. En algunas regiones, es posible que haya restricciones adicionales para los nombres de los buckets. Para obtener más información, consulte Restricciones y limitaciones de los buckets en la Guía del usuario de Amazon S3.
   b. En Región AWS , seleccione la región donde ha creado el equilibrador de carga.
   c. Para el cifrado predeterminado, elija las claves administradas por Amazon S3 (SSE-S3).
   d. Elija Crear bucket.

## Paso 2: Adjuntar una política al bucket de S3

El bucket de S3 debe tener una política que conceda permiso a Elastic Load Balancing para escribir los registros de acceso en el 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.

Si utiliza un bucket existente que ya tiene una política adjunta, puede agregar la instrucción para los registros de acceso de Elastic Load Balancing a la política. En este caso, recomendamos evaluar el conjunto de permisos resultante para asegurarse de que sean adecuados para los usuarios que necesitan obtener acceso al bucket en relación con los registros de acceso.

Políticas de bucket disponibles

La política de bucket que utilices dependerá de la zona Región de AWS y del tipo de zona.

Regiones disponibles a partir de agosto de 2022 en adelante

Esta política otorga permisos al servicio de entrega de registros especificado. Usa esta política para los balanceadores de carga en las siguientes regiones:

- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Taipéi)
- Asia-Pacífico (Tailandia)
- Oeste de Canadá (Calgary)
- Europa (España)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (EAU)
- México (central)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso con el formato que se muestra en la política de ejemplo. Incluya siempre el ID de cuenta de la cuenta con el balanceador de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que solo los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN que especifique dependerá de si planea incluir un prefijo al habilitar los registros de acceso en el paso 3.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Regiones disponibles antes de agosto de 2022

Esta política concede permisos al ID de cuenta de Elastic Load Balancing especificado. Usa esta política para los balanceadores de carga en las regiones que se indican a continuación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Para`Principal`, *`elb-account-id`* sustitúyalo por el ID de la cuenta de Elastic Load Balancing para la región del balanceador de carga:

- Este de EE. UU. (Norte de Virginia): 127311923021
- Este de EE. UU. (Ohio): 033677994240
- Oeste de EE. UU. (Norte de California): 027434742980
- Oeste de EE. UU. (Oregón): 797873946194
- África (Ciudad del Cabo): 098369216593
- Asia-Pacífico (Hong Kong): 754344448648
- Asia-Pacífico (Yakarta): 589379963580
- Asia-Pacífico (Bombay): 718504428378
- Asia-Pacífico (Osaka): 383597477331
- Asia-Pacífico (Seúl): 600734575887
- Asia Pacífico (Singapur): 114774131450
- Asia Pacífico (Sídney): 783225319266
- Asia Pacífico (Tokio): 582318560864
- Canadá (Centro): 985666609251
- Europa (Fráncfort): 054676820928
- Europa (Irlanda): 156460612806
- Europa (Londres): 652711504416
- Europa (Milán): 635631232127
- Europa (París): 009996457667

- Europa (Estocolmo): 897822967062
- Medio Oriente (Baréin): 076674570225
- América del Sur (São Paulo): 507241528517

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso con el formato que se muestra en la política de ejemplo. Incluya siempre el ID de cuenta de la cuenta con el balanceador de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que solo los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN que especifique dependerá de si planea incluir un prefijo al habilitar los registros de acceso en el paso 3.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

AWS GovCloud (US) Regiones

Esta política concede permisos al ID de cuenta de Elastic Load Balancing especificado. Usa esta política para los balanceadores de carga en las regiones. AWS GovCloud (US)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
```

```
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::amzn-s3-demo-bucket/prefix/
AWSLogs/123456789012/*"
    }
  ]
}
```

Para`Principal`, *`elb-account-id`* sustitúyalo por el ID de la cuenta de Elastic Load Balancing para la región del balanceador de carga:

- AWS GovCloud (US-Oeste) — 048591011584
- AWS GovCloud (EEUU-Este) — 190560391635

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso con el formato que se muestra en la política de ejemplo. Incluya siempre el ID de cuenta de la cuenta con el balanceador de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que solo los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN del bucket de S3 que especifique depende de si planea incluir un prefijo al habilitar el paso 3 del enlace a los registros de acceso.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Zonas Outposts

La siguiente política otorga permisos al servicio de entrega de registros especificado. Utilice esta política para los equilibradores de carga en las zonas Outposts.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "logdelivery.elb.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
    }
}
```

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso con el formato que se muestra en la política de ejemplo. Incluya siempre el ID de cuenta de la cuenta con el balanceador de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que solo los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN del bucket de S3 que especifique depende de si planea incluir un prefijo al habilitar los registros de acceso en el paso 3.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

⚠ Incremento de la seguridad

Utilice las siguientes sugerencias para mejorar la seguridad de su bucket de S3.

Revise su política de buckets

- Utilice la ruta de recursos completa, incluida la parte del ID de cuenta del ARN del bucket de S3. No utilices caracteres comodín (*) en la parte del ID de cuenta del ARN del bucket de S3.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
```

- Úsalo `aws:SourceArn` para asegurarte de que solo los balanceadores de carga de la región y la cuenta especificadas puedan usar tu bucket.

```
"Condition": {
    "ArnLike": {
        "aws:SourceArn":
 "arn:aws:elasticloadbalancing:region:123456789012:loadbalancer/*"
    }
}
```

- `aws:SourceOrgId`aws:SourceArnUtilízalo con para asegurarte de que solo los balanceadores de carga de la organización especificada puedan usar tu bucket.

```
"Condition": {
    "StringEquals": {
        "aws:SourceOrgId": "o-1234567890"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    }
}
```

- Si tienes una `Deny` declaración que impide el acceso a las entidades principales de servicio excepto a las que estén explícitamente permitidas, asegúrate de añadirla `logdelivery.elasticloadbalancing.amazonaws.com` a la lista de entidades principales de servicio permitidas. Por ejemplo, si utilizó la `aws:PrincipalServiceNamesList` condición, añada `logdelivery.elasticloadbalancing.amazonaws.com` lo siguiente:

```
{
  "Effect": "Deny",
  "Principal": "*",
  "Condition": {
      "StringNotEqualsIfExists": {
          "aws:PrincipalServiceNamesList": [
```

```
                "logdelivery.elasticloadbalancing.amazonaws.com",
                "service.amazonaws.com"
            ]
        }
    }
}
```

Si ha utilizado el `NotPrincipal` elemento, añada `logdelivery.elasticloadbalancing.amazonaws.com` lo siguiente. Tenga en cuenta que le recomendamos que utilice la clave de `aws:PrincipalServiceNamesList` condición `aws:PrincipalServiceName` o para permitir explícitamente a los directores de servicio en lugar de utilizar el `NotPrincipal` elemento. Para obtener más información, consulte NotPrincipal.

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "service.amazonaws.com"
    ]
  }
},
```

Para adjuntar una política de bucket para los registros de acceso a su bucket con la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Seleccione el nombre del bucket para abrir la página de detalles.
3. Elija Permisos y, a continuación, seleccione Política de bucket, Editar.
4. Actualice la política de bucket para conceder los permisos necesarios.
5. Elija Guardar cambios.

## Paso 3: configurar los registros de acceso

Utilice el siguiente procedimiento para configurar los registros de acceso para capturar información de solicitudes y entregar los archivos de registro al bucket de S3.

Requisitos

El bucket debe cumplir los requisitos descritos en el paso 1 y debe adjuntar una política de bucket tal como se describe en el paso 2. Si incluye un prefijo, no debe incluir la cadena "»AWSLogs.

Para habilitar los registros de acceso para el equilibrador de carga desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Para la Monitorización, active los registros de acceso.
6. En URI de S3, ingrese el URI de S3 correspondiente a los archivos de registro. El URI que especifique depende de si utiliza un prefijo.
   - URI con el prefijo: s3:///*amzn-s3-demo-logging-bucket*`logging-prefix`
   - URI sin prefijo: s3://*amzn-s3-demo-logging-bucket*
7. Seleccione Save changes (Guardar cambios).

Para habilitar los registros de acceso mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes.

Para administrar el bucket de S3 para los registros de acceso

Asegúrese de deshabilitar los registros de acceso antes de eliminar el bucket que configuró para los registros de acceso. De lo contrario, si existe un nuevo bucket con el mismo nombre y la política de bucket requerida pero creada en una Cuenta de AWS que no le pertenece, Elastic Load Balancing podría escribir los registros de acceso del equilibrador de carga en este nuevo bucket.

## Paso 4: verificar los permisos del bucket

Después de habilitar los registros de acceso para el equilibrador de carga, Elastic Load Balancing valida el bucket de S3 y crea un archivo de prueba para garantizar que la política del bucket especifica los permisos necesarios. Puede utilizar la consola de Amazon S3 para comprobar que se ha creado el archivo de prueba. El archivo de prueba no es un archivo de registro de acceso real; no contiene registros de ejemplo.

Comprobación de la creación de un archivo de prueba en su bucket mediante la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Seleccione el nombre del bucket que especificó para los registros de acceso.
3. Vaya al archivo registro de prueba, `ELBAccessLogTestFile`. La ubicación depende de si utiliza un prefijo.

   - Ubicación con un prefijo:*amzn-s3-demo-logging-bucket*//*logging-prefix*/AWSLogs/*123456789012*ELBAccessLogTestFile
   - Ubicación sin prefijo:*amzn-s3-demo-logging-bucket*///AWSLogs*123456789012*ELBAccessLogTestFile

### Solución de problemas

Si recibe un error de acceso denegado, estas pueden ser causas posibles:

- La política del bucket no concede permiso a Elastic Load Balancing para escribir registros de acceso en el bucket. Compruebe que está utilizando la política de bucket correcta para la región. Compruebe que el ARN del recurso utilice el mismo nombre de bucket que especificó al habilitar los registros de acceso. Compruebe que el ARN del recurso no incluya un prefijo si no especificó un prefijo al habilitar los registros de acceso.
- El bucket usa una opción de cifrado del lado del servidor no compatible. El bucket debe usar claves administradas por Amazon S3 (SSE-S3).

## Registros de acceso deshabilitados del Equilibrador de carga de aplicación

Se íedem deshabilitar los registros de acceso del equilibrador de carga en cualquier momento. Después de deshabilitar los registros de acceso, los registros de acceso permanecerán en el bucket de S3 hasta que los elimine. Para obtener más información, consulte Crear, configurar y trabajar con buckets S3 en la Guía del usuario de Amazon S3.

Desactivar el registro de acceso desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.

4. En la pestaña Atributos, seleccione Editar.
5. Para la Monitorización, desactive los registros de acceso.
6. Seleccione Save changes (Guardar cambios).

Para deshabilitar los registros de acceso mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes.

# Registros de conexión del Equilibrador de carga de aplicación

Elastic Load Balancing proporciona registros de conexión que capturan información detallada sobre las solicitudes enviadas al equilibrador de carga. Cada registro contiene información como la dirección IP y el puerto del cliente, el puerto de oyente, el cifrado y el protocolo TLS que se usen, la latencia del protocolo de enlace TLS, el estado de la conexión y los detalles del certificado del cliente. Puede utilizar estos registros de conexión para analizar los patrones de solicitud y solucionar problemas.

Los registros de conexión son una característica opcional de Elastic Load Balancing que está desactivada de forma predeterminada. Una vez que se han habilitado los registros de conexión del equilibrador de carga, Elastic Load Balancing captura los registros y los almacena en el bucket de Amazon S3 que haya especificado como archivos comprimidos. Puede deshabilitar los registros de conexión en cualquier momento.

Se cobran los costos de almacenamiento en Amazon S3, pero no el ancho de banda que Elastic Load Balancing utilice para enviar los archivos de registros a Amazon S3. Para obtener más información acerca de los costos de almacenamiento, consulte Precios de Amazon S3.

Contenido

# Archivos de los registros de conexión

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

Los nombres de archivo de los registros de conexión utilizan el siguiente formato:

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

bucket

Nombre del bucket de S3.

prefix

(Opcional) El prefijo (jerarquía lógica) del bucket. El prefijo que especifique no debe incluir la cadena `AWSLogs`. Para obtener más información, consulte Organizar objetos con prefijos.

`AWSLogs`

Agregamos la parte del nombre de archivo que comienza por `AWSLogs` después del nombre del bucket y el prefijo que especifique.

aws-account-id

El ID de AWS cuenta del propietario.

region

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

aaaa/mm/dd

La fecha de entrega del registro.

load-balancer-id

ID de recurso del equilibrador 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 en la zona horaria de Zulu o UTC.

ip-address

La dirección IP del nodo del equilibrador de carga que controló la solicitud. Si se trata de un equilibrador 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 archivo de registro con el prefijo:

```
s3://amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/
elasticloadbalancing/us-east-2/2022/05/01/
conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

A continuación, se muestra un ejemplo de nombre de archivo de registro sin un prefijo:

```
s3://amzn-s3-demo-logging-bucket/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2022/05/01/conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

Puede almacenar los archivos de registro en su 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 Gestión del ciclo de vida de los objetos en la Guía del usuario de Amazon S3.

## Entradas de registro de conexión

Cada intento de conexión tiene una entrada en un archivo de registro de conexión. La forma en que se envían las solicitudes de los clientes depende de si la conexión es persistente o no. Las conexiones no persistentes tienen una sola solicitud, lo que crea una entrada única en el registro de acceso y en el de conexión. Las conexiones persistentes tienen varias solicitudes, lo que crea varias entradas en el registro de acceso y una sola entrada en el registro de conexión.

Contenido



## Sintaxis

En la siguiente tabla se describen los campos de una entrada de registro de conexión, 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 |
|---|---|
| timestamp | La hora, en formato ISO 8601, a la que el equilibrador de carga estableció correctamente o no pudo establecer una conexión. |
| client_ip | Dirección IP del cliente solicitante. |
| client_port | Puerto del cliente solicitante. |
| listener_port | Puerto del oyente del equilibrador de carga que recibe la solicitud del cliente. |
| tls_protocol | [Listener de HTTPS] El SSL/TLS protocolo utilizado durante los apretones de manos. Este campo está configurado para no ser - solicitado. SSL/TLS |
| tls_cipher | [Listener HTTPS] El SSL/TLS protocolo utilizado durante los apretones de manos. Este campo está configurado para no ser - solicitado. SSL/TLS |
| tls_handshake_latency | [Oyente HTTPS] El tiempo total en segundos, con una precisión de milisegundos, transcurrido hasta que se estableció un protocolo de enlace correcto. Este campo está establecido como - cuando:<br>• La solicitud entrante no es una SSL/TLS solicitud.<br>• El protocolo de enlace no se ha establecido correctamente. |

| Campo | Descripción |
| --- | --- |
| leaf_client_cert_subject | [Oyente HTTPS] El nombre del asunto del certificado de cliente Leaf. Este campo está establecido como - cuando:<br>• La solicitud entrante no es una SSL/TLS solicitud.<br>• El oyente del equilibrador de carga no se ha configurado con mTLS activado.<br>• El servidor no puede obtener load/parse el certificado del cliente. |
| leaf_client_cert_validity | [Oyente HTTPS] La validez, con `not-before` y `not-after` en formato ISO 8601, del certificado de cliente Leaf. Este campo está establecido como - cuando:<br>• La solicitud entrante no es una SSL/TLS solicitud.<br>• El oyente del equilibrador de carga no se ha configurado con mTLS activado.<br>• El servidor no puede obtener load/parse el certificado del cliente. |
| leaf_client_cert_serial_number | [Oyente HTTPS] El número de serie del certificado de cliente Leaf. Este campo está establecido como - cuando:<br>• La solicitud entrante no es una SSL/TLS solicitud.<br>• El oyente del equilibrador de carga no se ha configurado con mTLS activado.<br>• El servidor no puede obtener load/parse el certificado del cliente. |
| tls_verify_status | [Oyente HTTPS] El estado de la solicitud de conexión. Este valor corresponde a `Success` si la conexión se estableció correctamente. En una conexión errónea, el valor es `Failed:$error_code` . |
| conn_trace_id | El identificador de trazabilidad de la conexión es un identificador opaco único que se utiliza para identificar cada conexión. Una vez establecida la conexión con un cliente, las solicitudes posteriores de este cliente contienen este identificador en sus respectivas entradas del registro de acceso. Este ID funciona como una clave externa para crear un enlace entre los registros de conexión y acceso. |

## Códigos de motivo de error

Si el equilibrador de carga no puede establecer una conexión, este almacena uno de los siguientes códigos de motivo de error en el registro de conexión.

| Código | Descripción |
| --- | --- |
| `ClientCertMaxChainDepthExceeded` | Se superó la profundidad máxima de la cadena de certificados de cliente. |
| `ClientCertMaxSizeExceeded` | Se superó el tamaño máximo del certificado de cliente. |
| `ClientCertCrlHit` | CA revocó el certificado de cliente. |
| `ClientCertCrlProcessingError` | Error de procesamiento de CRL. |
| `ClientCertUntrusted` | El certificado de cliente no es de confianza. |
| `ClientCertNotYetValid` | El certificado de cliente aún no es válido. |
| `ClientCertExpired` | El certificado ha vencido. |
| `ClientCertTypeUnsupported` | El tipo de certificado de cliente no es compatible. |
| `ClientCertInvalid` | El certificado de cliente no es válido. |

| Código | Descripción | |
|---|---|---|
| `ClientCertPurposeInvalid` | El propósito del certificado de cliente no es válido. | |
| `ClientCertRejected` | El certificado de cliente se rechazó mediante una validación de servidor personalizada. | |
| `UnmappedConnectionError` | Error de conexión en el tiempo de ejecución no asignado. | |

## Ejemplo de entradas de registro

A continuación, se muestran ejemplos de entradas de registro de conexión. Tenga en cuenta que el texto del ejemplo aparece en varias líneas solo para facilitar su lectura.

El siguiente es un ejemplo de entrada de registro para una conexión correcta con un agente de escucha HTTPS con el modo de verificación TLS mutua habilitado en el puerto 443.

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
 4.036
"CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z
FEF257372D5C14D4 Success TID_3180a73013c8ca4bac2f731159d4b0fe
```

El siguiente es un ejemplo de entrada de registro para una conexión fallida con un agente de escucha HTTPS con el modo de verificación TLS mutua habilitado en el puerto 443.

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
 -
"CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z
FEF257372D5C14D4 Failed:ClientCertUntrusted TID_1c71a68d70587445ad5127ff8b2687d7
```

## Procesamiento de archivos de registros de conexión

Los archivos de registros de conexión 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 equilibrador de carga puede generar archivos registro con gigabytes de datos. Es posible que no pueda procesar una cantidad tan grande de datos mediante line-by-line el procesamiento. 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 registros de conexión:

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Loggly
- Splunk
- Sumo Logic

## Habilitación de registros de conexión del Equilibrador de carga de aplicación

Al habilitar los registros de conexión del equilibrador de carga, debe especificar el nombre del bucket de S3 donde el equilibrador de carga almacenará los registros. El bucket debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir en el bucket.

Tareas

- Paso 1: Crear un bucket de S3
- Paso 2: Adjuntar una política al bucket de S3
- Paso 3: configurar registros de conexión
- Paso 4: verificar los permisos del bucket
- Solución de problemas

## Paso 1: Crear un bucket de S3

Al habilitar los registros de conexión, es preciso especificar un bucket de S3 para estos. Puede utilizar un bucket existente o crear uno específico para los registros de conexión. El bucket debe cumplir los siguientes requisitos.

Requisitos

- El bucket debe estar ubicado en la misma región que el equilibrador de carga. El bucket y el equilibrador de carga pueden ser propiedad de diferentes cuentas.
- La única opción de cifrado del lado del servidor que se admite son claves administradas por Amazon S3 (SSE-S3). Para obtener más información, consulte Claves de cifrado administradas por Amazon S3 (SSE-S3).

Para crear un bucket de S3 con la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Elija Crear bucket.
3. En la página Crear un bucket, realice las siguientes acciones:
    a. En Nombre del bucket, escriba un nombre para el bucket. Este nombre debe ser único entre todos los nombres de buckets de Amazon S3. En algunas regiones, es posible que haya restricciones adicionales para los nombres de los buckets. Para obtener más información, consulte Restricciones y limitaciones de los buckets en la Guía del usuario de Amazon S3.
    b. En Región AWS , seleccione la región donde ha creado el equilibrador de carga.
    c. Para el cifrado predeterminado, elija las claves administradas por Amazon S3 (SSE-S3).
    d. Elija Crear bucket.

## Paso 2: Adjuntar una política al bucket de S3

El bucket de S3 debe tener una política que conceda permiso a Elastic Load Balancing para escribir los registros de conexión en el 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.

Si utiliza un bucket existente que ya tiene una política adjunta, puede agregar la instrucción para los registros de conexión de Elastic Load Balancing a la política. En este caso, recomendamos evaluar

el conjunto de permisos resultante para asegurarse de que sean adecuados para los usuarios que necesitan obtener acceso al bucket en relación con los registros de conexión.

Políticas de bucket disponibles

La política de bucket que utilices dependerá de la zona Región de AWS y del tipo de zona.

⚠ Mejore la seguridad mediante el uso de un cubo S3 preciso ARNs.

- Utilice la ruta de recursos completa, no solo el ARN del bucket S3.
- Incluya la parte del ID de cuenta del ARN del bucket de S3.
- No utilices caracteres comodín (*) en la parte del ID de cuenta del ARN del bucket de S3.

Regiones disponibles a partir de agosto de 2022 en adelante

Esta política otorga permisos al servicio de entrega de registros especificado. Usa esta política para los balanceadores de carga en las siguientes regiones:

- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Tailandia)
- Oeste de Canadá (Calgary)
- Europa (España)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (EAU)
- México (central)

JSON

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso con el formato que se muestra en la política de ejemplo. Incluya siempre el ID de cuenta de la cuenta con el balanceador de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que solo los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN del bucket de S3 que especifique depende de si planea incluir un prefijo al habilitar los registros de acceso en el paso 3.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Uso de NotPrincipal cuando Effect es Deny

Si la política de bucket de Amazon S3 utiliza `Effect` con el valor `Deny` e incluye `NotPrincipal` tal como se muestra en el siguiente ejemplo, asegúrese de que `logdelivery.elasticloadbalancing.amazonaws.com` esté incluido en la lista `Service`.

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
    ]
  }
},
```

Regiones disponibles antes de agosto de 2022

Esta política concede permisos a la cuenta de Elastic Load Balancing especificada. Utilice esta política para los balanceadores de carga en las regiones que se indican a continuación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
       "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/
*"
    }
  ]
}
```

Para`Principal`, *`elb-account-id`* sustitúyalo por el ID de la cuenta de Elastic Load Balancing para la región del balanceador de carga:

- Este de EE. UU. (Norte de Virginia): 127311923021
- Este de EE. UU. (Ohio): 033677994240
- Oeste de EE. UU. (Norte de California): 027434742980
- Oeste de EE. UU. (Oregón): 797873946194

- África (Ciudad del Cabo): 098369216593
- Asia-Pacífico (Hong Kong): 754344448648
- Asia-Pacífico (Yakarta): 589379963580
- Asia-Pacífico (Bombay): 718504428378
- Asia-Pacífico (Osaka): 383597477331
- Asia-Pacífico (Seúl): 600734575887
- Asia Pacífico (Singapur): 114774131450
- Asia Pacífico (Sídney): 783225319266
- Asia Pacífico (Tokio): 582318560864
- Canadá (Centro): 985666609251
- Europa (Fráncfort): 054676820928
- Europa (Irlanda): 156460612806
- Europa (Londres): 652711504416
- Europa (Milán): 635631232127
- Europa (París): 009996457667
- Europa (Estocolmo): 897822967062
- Medio Oriente (Baréin): 076674570225
- América del Sur (São Paulo): 507241528517

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso con el formato que se muestra en la política de ejemplo. Incluya siempre el ID de cuenta de la cuenta con el balanceador de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que solo los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN del bucket de S3 que especifique depende de si planea incluir un prefijo al habilitar los registros de acceso en el paso 3.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

AWS GovCloud (US) Regiones

Esta política concede permisos a la cuenta de Elastic Load Balancing especificada. Usa esta política para los balanceadores de carga en las Zonas de Disponibilidad o en las Zonas Locales de las AWS GovCloud (US) regiones de la lista siguiente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws-us-gov:s3:::amzn-s3-demo-bucket/prefix/
AWSLogs/123456789012/*"
    }
  ]
}
```

Para `Principal` *`elb-account-id`* reemplazarlo por el ID de la cuenta de Elastic Load Balancing para la región del balanceador de carga:

- AWS GovCloud (US-Oeste) — 048591011584
- AWS GovCloud (EEUU-Este) — 190560391635

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso con el formato que se muestra en la política de ejemplo. Incluya siempre el ID de cuenta de la cuenta con el balanceador

de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN del bucket de S3 que especifique depende de si planea incluir un prefijo al habilitar los registros de acceso.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Zonas Outposts

La siguiente política otorga permisos al servicio de entrega de registros especificado. Utilice esta política para los equilibradores de carga en las zonas Outposts.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "logdelivery.elb.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/123456789012/*"
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
    }
}
```

Para`Resource`, introduzca el ARN de la ubicación de los registros de acceso. Incluya siempre el ID de cuenta de la cuenta con el balanceador de carga en la ruta de recursos del ARN del bucket de

S3. Esto garantiza que solo los balanceadores de carga de la cuenta especificada puedan escribir registros de acceso en el bucket de S3.

El ARN que especifique dependerá de si planea incluir un prefijo al habilitar los registros de acceso en el paso 3.

Ejemplo de ARN del bucket de S3 con un prefijo

El nombre del bucket de S3 es amzn-s3-demo-logging-bucket y el prefijo es. logging-prefix

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/logging-prefix/AWSLogs/123456789012/*
```

Ejemplo de ARN del bucket de S3 sin prefijo

El nombre del depósito de S3 esamzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

Uso de NotPrincipal cuando Effect es Deny

Si la política de bucket de Amazon S3 utiliza `Effect` con el valor `Deny` e incluye `NotPrincipal` tal como se muestra en el siguiente ejemplo, asegúrese de que `logdelivery.elasticloadbalancing.amazonaws.com` esté incluido en la lista `Service`.

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
    ]
  }
},
```

Incorporación de una política de bucket para los registros de conexión a su bucket con la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Seleccione el nombre del bucket para abrir la página de detalles.
3. Elija Permisos y, a continuación, seleccione Política de bucket, Editar.

4. Actualice la política de bucket para conceder los permisos necesarios.
5. Seleccione Save changes (Guardar cambios).

## Paso 3: configurar registros de conexión

Utilice el siguiente procedimiento para configurar los registros de conexión a fin de capturar y entregar los archivos de registro al bucket de S3.

Requisitos

El bucket debe cumplir los requisitos descritos en el paso 1 y debe adjuntar una política de bucket tal como se describe en el paso 2. Si especifica un prefijo, no debe incluir la cadena "». AWSLogs

Habilitación de los registros de conexión para el equilibrador de carga desde la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En Supervisión, active los registros de conexión.
6. En URI de S3, ingrese el URI de S3 correspondiente a los archivos de registro. El URI que especifique depende de si utiliza un prefijo.
   - URI con un prefijo: `s3://bucket-name/prefix`
   - URI sin un prefijo: `s3://bucket-name`
7. Seleccione Save changes (Guardar cambios).

Para habilitar los registros de conexión mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes.

Administración del bucket de S3 para los registros de conexión

Asegúrese de deshabilitar los registros de conexión antes de eliminar el bucket que configuró para los registros de conexión. De lo contrario, si existe un nuevo bucket con el mismo nombre y la política de bucket requerida pero que se creó en una Cuenta de AWS que no le pertenece, Elastic Load Balancing podría escribir los registros de conexión del equilibrador de carga en este nuevo bucket.

### Paso 4: verificar los permisos del bucket

Después de habilitar los registros de conexión en el equilibrador de carga, Elastic Load Balancing valida el bucket de S3 y crea un archivo de prueba para garantizar que la política del bucket especifica los permisos necesarios. Puede utilizar la consola de Amazon S3 para comprobar que se ha creado el archivo de prueba. El archivo de prueba no es un archivo de registro de conexión real; no contiene registros de ejemplo.

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

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Seleccione el nombre del bucket que especificó para los registros de conexión.
3. Vaya al archivo registro de prueba, `ELBConnectionLogTestFile`. La ubicación depende de si utiliza un prefijo.

   - Ubicación con un prefijo:*amzn-s3-demo-logging-bucket*//*prefix*/AWSLogs/*123456789012*ELBConnectionLogTestFile
   - Ubicación sin prefijo:*amzn-s3-demo-logging-bucket*///AWSLogs*123456789012*ELBConnectionLogTestFile

### Solución de problemas

Si recibe un error de acceso denegado, estas pueden ser causas posibles:

- La política del bucket no concede permiso a Elastic Load Balancing para escribir registros de conexión en el bucket. Compruebe que está utilizando la política de bucket correcta para la región. Compruebe que el ARN del recurso utilice el mismo nombre de bucket que especificó al habilitar los registros de conexión. Compruebe que el ARN del recurso no incluya un prefijo si no especificó un prefijo al habilitar los registros de conexión.
- El bucket usa una opción de cifrado del lado del servidor no compatible. El bucket debe usar claves administradas por Amazon S3 (SSE-S3).

## Deshabilitar los registros de conexión del Equilibrador de carga de aplicación

Puede deshabilitar los registros de conexión del equilibrador de carga en cualquier momento. Después de deshabilitar los registros de conexión, estos permanecerán en el bucket de S3 hasta que

los elimine. Para obtener más información, consulte Crear, configurar y trabajar con buckets en la Guía del usuario de Amazon S3.

Deshabilitar los registros de conexión mediante la consola

1. Abre la EC2 consola de Amazon en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En Supervisión, desactive los registros de conexión.
6. Seleccione Save changes (Guardar cambios).

Para deshabilitar los registros de conexión mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes.

# Solicite un rastreo de equilibrador de carga de aplicaciones.

Cuando el equilibrador 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 equilibrador de carga y el destino también pueden agregar o actualizar este encabezado.

Puede utilizar el rastreo de solicitudes para realizar el seguimiento de las solicitudes HTTP de los clientes a los destinos u otros servicios. Si habilita los registros de acceso, se registra el contenido del encabezado X-Amzn-Trace-Id. Para obtener más información, consulte Registros de acceso del Equilibrador de carga de aplicación.

## 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 equilibrador de carga conserva estos campos, pero no los utiliza.

versión

Número de versión. Este valor es 1.

hora

Tiempo en formato de tiempo Unix, en segundos. Este valor tiene 8 dígitos hexadecimales.

id

Identificador de rastreo. Este valor es de 24 dígitos hexadecimales.

Ejemplos

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

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

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

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

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

## Limitaciones

- El equilibrador 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 equilibrador de carga vuelve a escribir el encabezado X-Amzn-Trace-Id con un campo `Root` .
- Con WebSockets, solo puede realizar un seguimiento hasta que la solicitud de actualización se haya realizado correctamente.

# Solución de problemas de Equilibrador de carga de aplicación

La siguiente información puede ayudarle a solucionar problemas del Equilibrador de carga de aplicación.

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 destinos del Equilibrador de carga de aplicación..

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 equilibrador 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 equilibrador de carga. Además, el grupo de seguridad del equilibrador 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 equilibrador 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 equilibrador de carga está esperando y asegúrese de que la aplicación está configurada para devolver estos códigos de éxito.

El código de respuesta del destino tenía un formato incorrecto o se produjo un error al conectarse al destino

Comprueba que tu aplicación responde a las solicitudes de comprobación de estado del equilibrador de carga. Algunas aplicaciones requieren una configuración adicional para responder a las comprobaciones de estado, como una configuración de host virtual para responder al encabezado de host HTTP enviado por el equilibrador de carga. El valor del encabezado del host contiene la dirección IP privada del destino, seguida del puerto de comprobación de estado

cuando no se usa el puerto predeterminado. Si el destino usa un puerto de comprobación de estado, el valor del encabezado del host únicamente contiene la dirección IP privada del destino. Por ejemplo, si la dirección IP privada del destino es `10.0.0.10` y el puerto de comprobación de estado es `8080`, el encabezado del host HTTP que envía el equilibrador de carga en las comprobaciones de estado es `Host: 10.0.0.10:8080`. Si la dirección IP privada del destino es `10.0.0.10` y el puerto de comprobación de estado es `80`, el encabezado del host HTTP que envía el equilibrador de carga en las comprobaciones de estado es `Host: 10.0.0.10`. Es posible que se necesite una configuración de host virtual para responder a ese host, o una configuración predeterminada, para comprobar correctamente el estado de la aplicación. Las solicitudes de comprobación de estado tienen los siguientes atributos: `User-Agent` se establece en `ELB-HealthChecker/2.0`, el terminador de línea de los campos del encabezado del mensaje es la secuencia CRLF y el encabezado termina en la primera línea vacía seguida de un CRLF.

## Los clientes no pueden conectarse a un equilibrador de carga orientado a Internet

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

El equilibrador de carga expuesto a Internet está conectado a una subred privada

Debe especificar las subredes públicas para el equilibrador de carga. Una subred pública tiene una ruta hacia la puerta de enlace de Internet de la nube privada virtual (VPC).

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

El grupo de seguridad del balanceador de carga y cualquier red ACLs de las subredes del balanceador de carga deben permitir el tráfico entrante de los clientes y el tráfico saliente a los clientes en los puertos de escucha.

## El equilibrador de carga no recibe las solicitudes enviadas a un dominio personalizado

Si el equilibrador de carga no recibe las solicitudes enviadas a un dominio personalizado, compruebe lo siguiente:

El nombre de dominio personalizado no se resuelve en la dirección IP del equilibrador de carga

- Confirme en qué dirección IP se resuelve el nombre de dominio personalizado mediante una interfaz de línea de comandos.
  - Linux, macOS o Unix: puede utilizar el comando `dig` dentro de Terminal. Ej.`dig example.com`
  - Windows: puede utilizar el comando `nslookup` dentro del símbolo del sistema. Ej.`nslookup example.com`
- Confirme en qué dirección IP se resuelve el nombre de DNS del equilibrador de carga mediante una interfaz de línea de comandos.
- Compare ambos resultados. Las direcciones IP deben coincidir.

Si utiliza Route 53 para alojar su dominio personalizado, consulte Mi dominio no está disponible en Internet en la Guía para desarrolladores de Amazon Route 53.

## Las solicitudes HTTPS que se envían al equilibrador de carga devuelven “NET: :ERR_CERT_COMMON_NAME_INVALID”

Si las solicitudes HTTPS reciben `NET::ERR_CERT_COMMON_NAME_INVALID` del equilibrador de carga, compruebe las siguientes causas posibles:

- El nombre de dominio utilizado en la solicitud HTTPS no coincide con el nombre alternativo especificado en el certificado ACM asociado a los oyentes.
- Se utiliza el nombre de DNS predeterminado del equilibrador de carga. El nombre de DNS predeterminado no se puede utilizar para realizar solicitudes HTTPS, ya que no se puede solicitar un certificado público para el dominio `*.amazonaws.com`.

## El equilibrador de carga muestra tiempos de procesamiento elevados

El equilibrador de carga cuenta los tiempos de procesamiento de forma diferente según la configuración.

- Si AWS WAF está asociado a tu Application Load Balancer y un cliente envía una solicitud HTTP POST, el tiempo de envío de los datos de las solicitudes POST se refleja en el

`request_processing_time` campo de los registros de acceso al balanceador de carga. Este comportamiento se espera para solicitudes HTTP POST.

- Si no AWS WAF está asociado a tu Application Load Balancer y un cliente envía una solicitud HTTP POST, el tiempo de envío de los datos de las solicitudes POST se refleja en el `target_processing_time` campo de los registros de acceso al balanceador de carga. Este comportamiento se espera para solicitudes HTTP POST.

## El equilibrador de carga envía un código de respuesta 000

En el caso de las conexiones HTTP/2, si el número de solicitudes atendidas a través de una conexión supera las 10 000, el balanceador de cargas envía una trama GOAWAY y cierra la conexión con un TCP FIN.

## El equilibrador de carga genera un error HTTP

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

Errores

- HTTP 400: Solicitud errónea
- HTTP 401: No autorizado
- HTTP 403: Prohibido
- HTTP 405: Método no permitido
- HTTP 408: Request timeout
- HTTP 413: Carga demasiado grande
- HTTP 414: URI demasiado largo
- HTTP 460
- HTTP 463
- HTTP 464
- HTTP 500: Error interno del servidor
- HTTP 501: No implementado
- HTTP 502: Bad puerta de enlace
- HTTP 503: Service unavailable

- HTTP 504: Gateway timeout
- HTTP 505: Versión no compatible
- HTTP 507: almacenamiento insuficiente
- HTTP 561: No autorizado

## HTTP 400: Solicitud errónea

Causas posibles:

- El cliente envió una solicitud incorrecta que no se ajusta a la especificación de HTTP.
- El encabezado de la solicitud supera los 16 KB por línea de solicitud, los 16 KB por línea de encabezado o los 64 KB en el conjunto del encabezado.
- El cliente cerró la conexión antes de enviar el cuerpo completo de la solicitud.

## HTTP 401: No autorizado

Ha configurado una regla del oyente para autenticar a los usuarios, pero se cumple alguna de las condiciones siguientes:

- Configuró `OnUnauthenticatedRequest` para denegar el acceso a los usuarios no autenticados o el IdP denegó el acceso.
- El tamaño de las notificaciones devueltas por el IdP supera el tamaño máximo admitido por el equilibrador de carga.
- Un cliente ha enviado una solicitud HTTP/1.0 sin encabezado de host y el equilibrador de carga no pudo generar una URL de redirección.
- El ámbito de la solicitud no devuelve un token de ID.
- No se finaliza el proceso de inicio de sesión antes de que caduque el tiempo de espera para iniciar sesión del cliente. Para obtener más información, consulte Tiempo de espera para iniciar sesión en el cliente.

## HTTP 403: Prohibido

Configuró una lista de control de acceso AWS WAF web (ACL web) para monitorear las solicitudes a su Application Load Balancer y esta bloqueó una solicitud.

## HTTP 405: Método no permitido

El cliente utilizó el método TRACE, que no es compatible con el Equilibrador de carga de aplicación.

## 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

Causas posibles:

- El destino es una función de Lambda y el cuerpo de la solicitud supera 1 MB.
- El encabezado de la solicitud supera los 16 KB por línea de solicitud, los 16 KB por línea de encabezado o los 64 KB en el conjunto del encabezado.

## HTTP 414: URI demasiado largo

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

## HTTP 460

El equilibrador de carga recibió una solicitud de un cliente, pero el cliente cerró la conexión con el equilibrador 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 equilibrador 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 equilibrador de carga.

## HTTP 463

El equilibrador de carga recibió un encabezado de solicitud X-Forwarded-For con demasiadas direcciones IP. El límite máximo de direcciones IP es de 30.

## HTTP 464

El equilibrador de carga recibió un protocolo de solicitudes entrantes que no es compatible con la configuración de versiones del protocolo del grupo de destino.

Causas posibles:

- El protocolo de solicitud es HTTP/1.1, mientras que la versión del protocolo del grupo de destino es gRPC o HTTP/2.
- El protocolo de solicitud es un gRPC, mientras que la versión del protocolo del grupo de destino es un HTTP/1.1.
- El protocolo de solicitud es HTTP/2 y la solicitud no es POST, mientras que la versión del protocolo del grupo de destino es un gRPC.

## HTTP 500: Error interno del servidor

Causas posibles:

- Configuró una lista de control de acceso AWS WAF web (ACL web) y se produjo un error al ejecutar las reglas de la ACL web.
- El equilibrador de carga no puede comunicarse con el punto de conexión del token de IdP o el punto de conexión de información de usuario de IdP.
  - Compruebe que el DNS del IdP se pueda resolver públicamente.
  - Compruebe que los grupos de seguridad del equilibrador de carga y la red ACLs de la VPC permiten el acceso saliente a estos puntos de conexión.
  - Compruebe que la VPC tiene acceso a Internet. Si hay un equilibrador de carga interno, utilice una puerta de enlace NAT para permitirle que obtenga acceso a Internet.
- La reclamación del usuario recibida del IdP tiene un tamaño superior a 11 KB.
- El punto final del token de IdP o el punto final de información de usuario del IdP tardan más de 5 segundos en responder.

## HTTP 501: No implementado

El equilibrador 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 puerta de enlace

Causas posibles:

- El equilibrador de carga recibió un TCP RST desde el destino cuando intentó establecer una conexión.
- El equilibrador 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 equilibrador 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 equilibrador 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 equilibrador de carga.
- La respuesta del destino es incorrecta o contiene encabezados HTTP que no son válidos.
- El encabezado de respuesta destino superó los 32 K para todo el encabezado de respuesta.
- El período de retardo de anulación del registro para una solicitud que se maneja mediante un destino cuyo registro se ha anulado. Aumente el periodo de retraso de manera que las operaciones largas puedan completarse.
- El destino es una función de Lambda y el cuerpo de la respuesta supera 1 MB.
- El destino es una función de Lambda que no respondió antes de que se agotara el tiempo de espera configurado.
- El destino es una función de Lambda que ha devuelto un error o el servicio de Lambda ha limitado la función.
- El equilibrador de carga ha detectado un error de protocolo de enlace SSL al conectarse a un destino.

Para obtener más información, consulte Cómo solucionar los errores HTTP 502 del Application Load Balancer en el AWS Support Knowledge Center.

## HTTP 503: Service unavailable

Los grupos objetivo del balanceador de cargas no tienen destinos registrados o todos los objetivos registrados están en un mismo estado. `unused`

## HTTP 504: Gateway timeout

Causas posibles:

- El equilibrador de carga ha establecido una conexión con el destino antes de que se agotara el tiempo de espera de conexión (10 segundos).
- El equilibrador de carga estableció una conexión con el destino, pero el destino no respondió antes de que transcurriera el período de inactividad.
- La ACL o las SecurityGroup políticas de la red no permitían el tráfico desde los destinos a los nodos del equilibrador 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 equilibrador de carga agotó el tiempo de espera con los bytes restantes.
- El destino es una función de Lambda y el servicio Lambda no respondió antes de que expirara el tiempo de espera de conexión.
- El equilibrador de carga ha detectado un error de tiempo de espera del protocolo de enlace SSL (10 segundos) al conectarse a un destino.

## HTTP 505: Versión no compatible

El equilibrador de carga recibió una solicitud de versión HTTP inesperada. Por ejemplo, el equilibrador de carga estableció una conexión HTTP/1 pero recibió una solicitud HTTP/2.

## HTTP 507: almacenamiento insuficiente

La URL de redirección es demasiado larga.

## HTTP 561: No autorizado

Configuró una regla de oyente para autenticar a los usuarios, pero el IdP devolvió un código de error al autenticar al usuario. Compruebe en sus registros de acceso el código de motivo de error correspondiente.

# Hay un destino que genera un error HTTP

El equilibrador 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`.

# No AWS Certificate Manager hay ningún certificado disponible para su uso

Si decide utilizar un agente de escucha HTTPS con su Application Load Balancer AWS Certificate Manager , debe validar la propiedad del dominio antes de emitir un certificado. Si se omite este paso durante la configuración, el certificado permanece en el estado `Pending Validation` y no estará disponible para su uso hasta que se valide.

- Si utiliza la validación por correo electrónico, consulte Validación por correo electrónico en la Guía del usuario de AWS Certificate Manager .
- Si utiliza la validación por correo electrónico, consulte Validación DNS en la Guía del usuario de AWS Certificate Manager .

# No se admiten encabezados de varias líneas

Los equilibradores de carga de aplicaciones no admiten encabezados multilínea, incluido el encabezado de tipo de medio `message/http`. Cuando se proporciona un encabezado multilínea, el Equilibrador de carga de aplicación añade un carácter de dos puntos, "`:`", antes de pasarlo al destino.

# Solución de problemas de destinos en mal estado mediante el mapa de recursos

Si los destinos del Equilibrador de carga de aplicación no superan las comprobaciones de estado, puede utilizar el mapa de recursos para buscar destinos en mal estado y tomar medidas en función del código del motivo del error. Para obtener más información, consulte Visualización del mapa de recursos del Equilibrador de carga de aplicación.

El mapa de recursos ofrece dos vistas: Información general y Mapa de destinos en mal estado. La información general se selecciona de forma predeterminada y muestra todos los recursos del equilibrador de carga. Si selecciona la vista Mapa de destinos en mal estado, solo se mostrarán los destinos en mal estado de cada grupo de destino asociado al Equilibrador de carga de aplicación.

> **Note**
>
> La opción Mostrar detalles del recurso debe estar habilitada para ver el resumen de la comprobación de estado y los mensajes de error de todos los recursos aplicables del mapa de recursos. Si no está habilitada, debe seleccionar cada recurso para ver sus detalles.

La columna Grupos de destino muestra un resumen de los destinos en buen y mal estado de cada grupo de destino. Esto puede ayudar a determinar si ninguno de los destinos está superando las comprobaciones de estado, o si son solo destinos concretos los que no las superan. Si ninguno de los destinos de un grupo de destino supera las comprobaciones de estado, revise la configuración del grupo de destino. Seleccione el nombre de un grupo de destino para abrir su página de detalles en una pestaña nueva.

La columna Destinos muestra el ID de destino y el estado actual de la comprobación de estado de cada destino. Cuando un destino no está en buen estado, se muestra el código del motivo del error de la comprobación de estado. Cuando sea un único destino el que no supera una comprobación de estado, verifique que el destino tiene recursos suficientes y confirme que las aplicaciones que se ejecutan en el destino estén disponibles. Seleccione el ID de un destino para abrir su página de detalles en una pestaña nueva.

Al seleccionar Exportar, tiene la opción de exportar la vista actual del mapa de recursos de su Equilibrador de carga de aplicación en formato PDF.

Verifique que la instancia no está superando las comprobaciones de estado y luego, en función del código del motivo del error, revise lo siguiente:

- Mal estado: la respuesta HTTP no coincide
  - Compruebe que la aplicación que se ejecuta en el destino envíe la respuesta HTTP correcta a las solicitudes de comprobación de estado del Equilibrador de carga de aplicación.
  - Como alternativa, puede actualizar la solicitud de comprobación de estado del Equilibrador de carga de aplicación para que coincida con la respuesta de la aplicación que se ejecuta en el destino.
- Mal estado: tiempo de espera de la solicitud agotado
  - Compruebe que los grupos de seguridad y las listas de control de acceso (ACL) de la red asociados a los destinos y al Equilibrador de carga de aplicación no están bloqueando la conectividad.

- Compruebe que el destino tenga suficientes recursos disponibles para aceptar conexiones desde el Equilibrador de carga de aplicación.
- Compruebe el estado de todas las aplicaciones que se ejecuten en el destino.
- Las respuestas a las comprobaciones de estado del Equilibrador de carga de aplicación se pueden ver en los registros de aplicaciones de cada destino. Para obtener más información, consulte Códigos de motivo de comprobación de estado.

- Insalubre: FailedHealthChecks
  - Compruebe el estado de todas las aplicaciones que se ejecuten en el destino.
  - Compruebe que el destino esté escuchando el tráfico en el puerto de la comprobación de estado.

> **Cuando se utiliza un oyente HTTPS**
>
> Puede seleccionar qué política de seguridad se utiliza para las conexiones frontend. La política de seguridad utilizada para las conexiones backend se selecciona automáticamente en función de la política de seguridad frontend que se utilice.
>
> - Si el oyente HTTPS utiliza una política de seguridad de TLS 1.3 para las conexiones frontend, se utiliza la política de seguridad `ELBSecurityPolicy-TLS13-1-0-2021-06` para las conexiones de back-end.
> - Si el oyente HTTPS no utiliza una política de seguridad de TLS 1.3 para las conexiones frontend, se utiliza la política de seguridad `ELBSecurityPolicy-2016-08` para las conexiones de back-end.
>
> Para obtener más información, consulte Políticas de seguridad.

  - Compruebe que el destino proporciona un certificado de servidor y una clave con el formato correcto especificado en la política de seguridad.
  - Compruebe que el destino admite uno o varios cifrados coincidentes y un protocolo que proporciona el Equilibrador de carga de aplicación para establecer protocolos de enlace TLS.

# Cuotas de los equilibradores de carga de aplicaciones

Tu AWS cuenta tiene cuotas predeterminadas, antes denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de los equilibradores de carga de aplicaciones, abra la consola de Service Quotas. En el panel de navegación, seleccione Servicios de AWS y elija Elastic Load Balancing. También puedes usar el comando describe-account-limits(AWS CLI) para Elastic Load Balancing.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas. Si la cuota aún no está disponible en Service Quotas, envíe una solicitud de aumento de la cuota de servicio.

Cuotas

- Equilibradores de carga
- Grupos de destino
- Reglas
- Almacenes de confianza
- Certificados
- Encabezados HTTP
- Unidades de capacidad del Load Balancer

## Equilibradores de carga

Su AWS cuenta tiene las siguientes cuotas relacionadas con los balanceadores de carga de aplicaciones.

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Equilibradores de carga de aplicaciones por región | 50 | Sí |
| Certificados por Equilibrador de carga de aplicación (sin incluir los certificados predeterminados) | 25 | Sí |

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Oyentes por Equilibrador de carga de aplicación | 50 | Sí |
| Grupos destino por acción por Equilibrador de carga de aplicación | 5 | No |
| Grupos de destino por equilibrador de carga de aplicaciones | 100 | No |
| Destinos por Equilibrador de carga de aplicación | 1 000 | Sí |

## Grupos de destino

Las cuotas siguientes son para grupos de destino.

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Grupos de destino por región | 3000* | Sí |
| Destinos por grupo de destino por región (instancias o direcciones IP) | 1 000 | Sí |
| Destinos por grupo de destino por región (funciones de Lambda) | 1 | No |
| Equilibradores de carga por grupo de destino | 1 | No |

* Esta cuota se comparte entre los equilibradores de carga de aplicaciones y los Equilibradores de carga de red.

## Reglas

Las siguientes cuotas son para reglas.

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Reglas por Equilibrador de carga de aplicación (no se incluyen las reglas predeterminadas) | 100 | Sí |
| Valores de condición por regla | 5 | No |
| Caracteres comodín de condición por regla | 5 | No |
| Evaluaciones de coincidencia por regla | 5 | No |

## Almacenes de confianza

Las siguientes cuotas son para almacenes de confianza.

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Almacenes de confianza por cuenta | 20 | Sí |
| Número de oyentes que utilizan mTLS en modo de verificación, por equilibrador de carga. | 2 | No |

## Certificados

Las siguientes cuotas se aplican a los certificados, incluida la publicidad de los nombres de los certificados de CA y las listas de revocación de certificados.

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Tamaño del certificado de CA | 16 KB | No |
| Número de certificados de CA por almacén de confianza | 25 | Sí |

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Tamaño del asunto de los certificados de CA por almacén de confianza | 10 000 | Sí |
| Profundidad máxima de la cadena de certificados | 4 | No |
| Entradas de revocación por almacén de confianza | 500.000 | Sí |
| Tamaño del archivo de la lista de revocación | 50 MB | No |
| Listas de revocación por almacén de confianza | 30 | Sí |
| Tamaño del mensaje TLS | 64 K | No |

## Encabezados HTTP

A continuación se presentan los límites de tamaño para los encabezados HTTP.

| Nombre | Valor predeterminado | Ajustable |
|---|---|---|
| Línea de solicitud | 16 K | No |
| Encabezado único | 16 K | No |
| Encabezado de respuesta completo | 32 K | No |
| Encabezado de solicitud completo | 64 K | No |

## Unidades de capacidad del Load Balancer

Las siguientes cuotas son para las unidades de capacidad del Load Balancer (LCU).

| Nombre | Valor predeterminado | Ajustable |
| --- | --- | --- |
| Unidades de capacidad reservadas para el Application Load Balancer (LCUs) por cada Application Load Balancer | 15.000 | Sí |
| Unidades de capacidad (LCU) de Application Load Balancer reservadas por región | 0 | Sí |

# Historial de revisión de los equilibrador de carga de aplicaciones

En la tabla siguiente, se describen las versiones de los equilibradores de carga de aplicaciones.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Modificación del encabezado HTTP | Esta versión añade compatibilidad con la modificación del encabezado HTTP en todos los códigos de respuesta. Anteriormente, esta función estaba limitada a los códigos de respuesta 2xx y 3xx. | 28 de febrero de 2025 |
| Reserva de unidades de capacidad | Esta versión añade compatibilidad para establecer una capacidad mínima para el balanceador de carga. | 20 de noviembre de 2024 |
| Mapa de recursos | Esta versión agrega compatibilidad para ver los recursos y las relaciones del equilibrador de carga en un formato visual. | 8 de marzo de 2024 |
| WAF en un clic | Esta versión añade soporte para configurar el comportamiento del balanceador de carga si se integra con un solo clic. AWS WAF | 6 de febrero de 2024 |
| TLS mutua | Esta versión agrega compatibilidad con la autenticación de TLS mutua. | 26 de noviembre de 2023 |

| | | |
|---|---|---|
| Pesos de destino automáticos | Esta versión agrega compatibilidad con el algoritmo de pesos de destino automáticos. | 26 de noviembre de 2023 |
| Finalización de TLS con FIPS 140-3 | Esta versión agrega políticas de seguridad que utilizan módulos criptográficos FIPS 140-3 cuando se finalizan conexiones TLS. | 20 de noviembre de 2023 |
| Registre los objetivos mediante IPv6 | Esta versión añade compatibilidad con el registro de instancias como destinos cuando se trata de IPv6. | 2 de octubre de 2023 |
| Políticas de seguridad que admiten TLS 1.3 | Esta versión agrega compatibilidad para las políticas de seguridad predefinidas de TLS 1.3. | 22 de marzo de 2023 |
| Cambio de zona | Esta versión agrega compatibilidad para desviar el tráfico de una única zona de disponibilidad dañada mediante la integración con Controlador de recuperación de aplicaciones (ARC) de Amazon. | 28 de noviembre de 2022 |
| Deshabilitar el equilibrio de carga entre zonas | Esta versión agrega compatibilidad para desactivar el equilibrador de carga entre zonas. | 28 de noviembre de 2022 |

| | | |
|---|---|---|
| Estado del grupo de destino | Esta versión permite configurar el recuento o el porcentaje mínimo de destinos que deben estar en buen estado y las acciones que debe realizar el equilibrador de carga cuando no se alcanza el umbral. | 28 de noviembre de 2022 |
| Equilibrio de carga entre zonas | Esta versión agrega compatibilidad para configurar el equilibrio de carga entre zonas en el nivel del grupo de destino. | 17 de noviembre de 2022 |
| IPv6 grupos objetivo | Esta versión añade compatibilidad con la configuración de grupos de IPv6 destino para los balanceadores de carga de aplicaciones. | 23 de noviembre de 2021 |
| IPv6 balanceadores de carga internos | Esta versión añade soporte para configurar grupos de IPv6 destino para los balanceadores de carga de aplicaciones. | 23 de noviembre de 2021 |
| AWS PrivateLink y direcciones IP estáticas | Esta versión admite el uso AWS PrivateLink y la exposición de direcciones IP estáticas al reenviar el tráfico directamente desde los balanceadores de carga de red a los balanceadores de carga de aplicaciones. | 27 de septiembre de 2021 |

| | | |
|---|---|---|
| Preservación del puerto del cliente | Esta versión agrega un atributo para preservar el puerto de origen que el cliente utiliza para conectarse al equilibrador de carga. | 29 de julio de 2021 |
| Encabezados TLS | Esta versión agrega un atributo para indicar que los encabezados TLS, que contienen información sobre la versión de TLS negociada y el conjunto de cifrado, se agregan a la solicitud del cliente antes de enviarla al destino. | 21 de julio de 2021 |
| Certificados de ACM adicionales | Esta versión es compatible con los certificados RSA con longitudes de clave de 2048, 3072 y 4096 bits, y con todos los certificados ECDSA. | 14 de julio de 2021 |
| Persistencia en función de la aplicación | En esta versión, se añade una cookie en función de aplicaciones para admitir sesiones persistentes en el equilibrador de carga. | 8 de febrero de 2021 |
| Política de seguridad para FS compatible con la versión 1.2 de TLS | Esta versión incorpora una política de seguridad para Forward Secrecy (FS) compatible con la versión 1.2 de TLS. | 24 de noviembre de 2020 |

| | | |
|---|---|---|
| No se puede abrir el soporte para WAF | Esta versión añade soporte para configurar el comportamiento del balanceador de cargas si se integra con él. AWS WAF | 13 de noviembre de 2020 |
| Compatibilidad con gRPC y HTTP/2 | Esta versión añade compatibilidad con cargas de trabajo de gRPC y HTTP/2. end-to-end | 29 de octubre de 2020 |
| Soporte para Outpost | Puede aprovisionar un Equilibrador de carga de aplicación en AWS Outposts. | 8 de septiembre de 2020 |
| Modo de mitigación de desincronización | En esta versión se agrega compatibilidad con el modo de mitigación de desincronización. | 17 de agosto de 2020 |
| Solicitudes menos pendientes | Esta versión añade soporte para el algoritmo de solicitudes menos pendientes. | 25 de noviembre de 2019 |
| Grupos de destino ponderados | Esta versión incorpora compatibilidad con acciones de reenvío con varios grupos de destino. Las solicitudes se distribuyen a estos grupos de destino en función de la ponderación especificada para cada grupo de destino. | 19 de noviembre de 2019 |
| New attribute (Nuevo atributo) | Esta versión incorpora compatibilidad con el atributo routing.http.drop_invalid_header_fields.enabled. | 15 de noviembre de 2019 |

| | | |
|---|---|---|
| Políticas de seguridad para FS | Esta versión agrega compatibilidad para tres políticas de seguridad de secreto hacia adelante predefinidas adicionales. | 8 de octubre de 2019 |
| Direccionamiento de solicitudes avanzado | Esta versión añade compatibilidad para tipos de condición adicionales para las reglas de oyente. | 27 de marzo de 2019 |
| Funciones de Lambda como destino | Esta versión añade compatibilidad para registrar funciones de Lambda como destino. | 29 de noviembre de 2018 |
| Acciones de redirección | Esta versión incorpora la compatibilidad con el equilibrador de carga para redirigir las solicitudes a una URL diferente. | 25 de julio de 2018 |
| Acciones de respuesta fija | Esta versión incorpora la compatibilidad con el equilibrador de carga para devolver una respuesta HTTP personalizada. | 25 de julio de 2018 |
| Políticas de seguridad para FS y TLS 1.2 | Esta versión añade soporte para dos políticas de seguridad predefinidas adicionales. | 6 de junio de 2018 |

| | | |
|---|---|---|
| Autenticación del usuario | Esta versión añade soporte para que el equilibrador de carga pueda autenticar a los usuarios de sus aplicaciones utilizando sus identidades corporativas o sociales antes de las solicitudes de direccion amiento. | 30 de mayo de 2018 |
| Permisos de nivel de recursos | Esta versión añade soporte para permisos en el nivel de recursos y claves de condición de etiquetado. | 10 de mayo de 2018 |
| Modo de inicio lento | Esta versión añade soporte para el modo de inicio lento, que aumenta gradualmente la cuota de solicitudes que el equilibrador de carga envía a un destino recién registrado mientras se calienta. | 24 de marzo de 2018 |
| Compatibilidad con SNI | Esta versión incorpora soporte para Indicación de nombre de servidor (SNI). | 10 de octubre de 2017 |
| Direcciones IP como destinos | Esta versión añade soporte para registrar direcciones IP como destinos. | 31 de agosto de 2017 |
| Enrutamiento basado en host | Esta versión añade soporte para las solicitudes de direccionamiento basadas en los nombres de host del encabezado de host. | 5 de abril de 2017 |

| | | |
|---|---|---|
| Políticas de seguridad para TLS 1.1 y TLS 1.2 | En esta versión, se han añadido las políticas de seguridad de TLS 1.1 y TLS 1.2. | 6 de febrero de 2017 |
| IPv6 soporte | Esta versión añade compatibilidad con las IPv6 direcciones. | 25 de enero de 2017 |
| Rastreo de solicitudes | En esta versión se agrega compatibilidad con el rastreo de solicitudes. | 22 de noviembre de 2016 |
| Soporte de percentiles para la métrica TargetResponseTime | Esta versión añade compatibilidad con las nuevas estadísticas de percentiles admitidas por Amazon. CloudWatch | 17 de noviembre de 2016 |
| Tipo de equilibrador de carga nuevo | Esta versión de Elastic Load Balancing presenta los equilibradores de carga de aplicaciones. | 11 de agosto de 2016 |

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