



Equilibradores de carga clásicos

ELB



## ELB: Equilibradores de carga clásicos

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

# Table of Contents

¿Qué es un equilibrador de carga clásico? .....	1
Información general sobre equilibradores de carga clásicos .....	1
Ventajas .....	2
Cómo comenzar .....	3
Precios .....	3
Equilibradores de carga expuestos a Internet .....	4
Nombres de DNS públicos del equilibrador de carga .....	4
Creación de un equilibrador de carga expuesto a Internet .....	5
Antes de empezar .....	5
Cree un Classic Load Balancer con Consola de administración de AWS .....	6
Equilibradores de carga internos .....	9
Nombre DNS público del equilibrador de carga .....	10
Creación de un equilibrador de carga interno .....	11
Requisitos previos .....	11
Creación de un equilibrador de carga interno a través de la consola .....	11
Crea un balanceador de cargas interno con el AWS CLI .....	14
Configuración del equilibrador de carga .....	17
Tiempo de inactividad de conexión .....	18
Configuración del tiempo de inactividad desde la consola .....	19
Configuración del tiempo de inactividad desde la AWS CLI .....	19
Equilibrio de carga entre zonas .....	20
Habilitación del equilibrio de carga entre zonas .....	20
Desactivación del equilibrio de carga entre zonas .....	22
Drenaje de conexiones .....	24
Habilitación del drenaje de conexiones .....	25
Desactivación de drenaje de conexiones .....	26
Sesiones persistentes .....	27
Persistencia de las sesiones en función de la duración .....	28
Persistencia de las sesiones controlada por la aplicación .....	31
Modo de mitigación de desincronización .....	34
Clasificaciones .....	34
Modos .....	36
Modificación del modo de mitigación de desincronización .....	36
Protocolo de proxy .....	37

Encabezado Proxy Protocol .....	38
Requisitos previos para habilitar Proxy Protocol .....	38
Habilitación de Proxy Protocol desde la AWS CLI .....	39
Desactivación de Proxy Protocol desde la AWS CLI .....	41
Tags .....	42
Restricciones de las etiquetas .....	42
Añada una etiqueta .....	43
Eliminación de una etiqueta .....	43
Subredes y zonas .....	44
Requisitos .....	45
Configurar las subredes con la consola .....	45
Configurar subredes con la CLI .....	46
Grupos de seguridad .....	47
Reglas recomendadas para los grupos de seguridad del equilibrador de carga .....	48
Asignación de grupos de seguridad a través de la consola .....	49
Asigne grupos de seguridad mediante el AWS CLI .....	50
Red ACLs .....	50
Nombre de dominio personalizado .....	52
Asociación del nombre de dominio personalizado al nombre del equilibrador de carga .....	53
Uso de la conmutación por error de DNS de Route 53 para el equilibrador de carga .....	54
Desasociación del nombre de dominio personalizado del equilibrador de carga .....	55
Oyentes .....	56
Protocolos .....	56
Protocolo TCP/SSL .....	57
Protocolo HTTP/HTTPS .....	57
Oyentes HTTPS/SSL .....	58
Certificados de servidor SSL .....	58
Negociación SSL .....	59
Autenticación del servidor backend .....	59
Configuraciones de oyentes .....	59
Encabezados X-Forwarded .....	62
X-Forwarded-For .....	63
X-Forwarded-Proto .....	63
X-Forwarded-Port .....	64
Oyentes HTTPS .....	65
Certificados SSL/TLS .....	66

Cree o importe un certificado mediante SSL/TLS AWS Certificate Manager .....	67
Importe un certificado mediante IAM SSL/TLS .....	67
Configuraciones de negociación SSL .....	67
Políticas de seguridad .....	68
Protocolos SSL .....	69
Preferencia del orden del servidor .....	69
Cifrados SSL .....	69
Conjunto de cifrado para conexiones backend .....	73
Políticas de seguridad SSL predefinidas .....	74
Protocolos por política .....	75
Cifrados por política .....	76
Políticas por cifrado .....	81
Creación de un equilibrador de carga HTTPS .....	86
Requisitos previos .....	87
Creación de un equilibrador de carga HTTPS a través de la consola .....	88
Crea un balanceador de cargas HTTPS mediante el AWS CLI .....	92
Configuración de un oyente HTTPS .....	104
Requisitos previos .....	104
Agregado de un oyente HTTPS a través de la consola .....	105
Agrega un agente de escucha HTTPS mediante el AWS CLI .....	106
Reemplazo del certificado SSL .....	108
Reemplazo del certificado SSL a través de la consola .....	109
Reemplazo del certificado SSL a través de la AWS CLI .....	110
Actualización de la configuración de negociación SSL .....	111
Actualización de la configuración de negociación SSL a través de la consola .....	112
Actualice la configuración de negociación de SSL mediante el AWS CLI .....	113
Instancias registradas .....	118
Prácticas recomendadas para las instancias .....	118
Recomendaciones para su VPC .....	119
Registrar instancias con el equilibrador de carga .....	120
Registro de una instancia .....	121
Visualización de las instancias que se registran con el equilibrador de carga .....	122
Determinación del equilibrador de carga para una instancia registrada .....	122
Anulación del registro de una instancia .....	122
Comprobaciones de estado .....	123
Configuración de la comprobación de estado .....	124

Actualización de la configuración de la comprobación de estado .....	127
Comprobación del estado de las instancias .....	127
Solución de problemas de las comprobaciones de estado .....	128
Grupos de seguridad .....	128
Red ACLs .....	129
Monitoreo del equilibrador de carga .....	131
CloudWatch métricas .....	131
Métricas del Equilibrador de carga clásico .....	132
Dimensiones de las métricas de los equilibradores de carga clásicos .....	142
Estadísticas correspondientes a las métricas del Equilibrador de carga clásico .....	143
Consulta CloudWatch las métricas de tu balanceador de cargas .....	144
Registros de acceso .....	145
Archivos de registro de acceso .....	146
Entradas de los registros de acceso .....	148
Procesamiento de registros de acceso .....	153
Habilitar registros de acceso .....	153
Desactivación de los registros de acceso .....	160
Solución de problemas del equilibrador de carga .....	162
errores de API .....	164
CertificateNotFound: Indefinido .....	164
OutofService: Se ha producido un error transitorio .....	164
Errores de HTTP .....	165
HTTP 400: BAD_REQUEST .....	166
HTTP 405: METHOD_NOT_ALLOWED .....	166
HTTP 408: Request timeout .....	166
HTTP 502: Bad gateway .....	167
HTTP 503: Service unavailable .....	167
HTTP 504: Gateway timeout .....	168
Métricas de código de respuesta .....	168
HTTPCode_ELB_4XX .....	169
HTTPCode_ELB_5XX .....	169
HTTPCode_Backend_2xx .....	169
HTTPCode_Backend_3xx .....	170
HTTPCode_Backend_4xx .....	170
HTTPCode_Backend_5xx .....	170
Comprobaciones de estado .....	171

Error en la página de destino de la comprobación de estado .....	171
Se ha agotado el tiempo de espera de conexión a las instancias .....	172
Se produce un error al autenticar la clave pública .....	173
La instancia no recibe tráfico desde el equilibrador de carga .....	173
Los puertos de la instancia no están abiertos .....	174
Las instancias de un grupo de escalado automático no superan la comprobación de estado de ELB .....	174
Conectividad del cliente .....	175
Los clientes no pueden conectarse a un equilibrador de carga orientado a internet .....	175
El equilibrador de carga no recibe las solicitudes enviadas a un dominio personalizado .....	175
Las solicitudes HTTPS que se envían al equilibrador de carga devuelven "NET: :ERR_CERT_COMMON_NAME_INVALID" .....	176
Registro de instancias .....	176
Registrar una EC2 instancia tarda demasiado .....	177
No se puede registrar una instancia lanzada desde una AMI pagada .....	177
Cuotas .....	178
Historial de revisión .....	179
.....	clxxxix

# ¿Qué es un equilibrador de carga clásico?

## Note

Los equilibradores de carga clásicos son los equilibradores de carga de la generación anterior de ELB. Se recomienda que migre a un equilibrador de carga de la generación actual. Para obtener más información, consulte [Migrar el Equilibrador de carga clásico](#).

ELB 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. ELB 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.

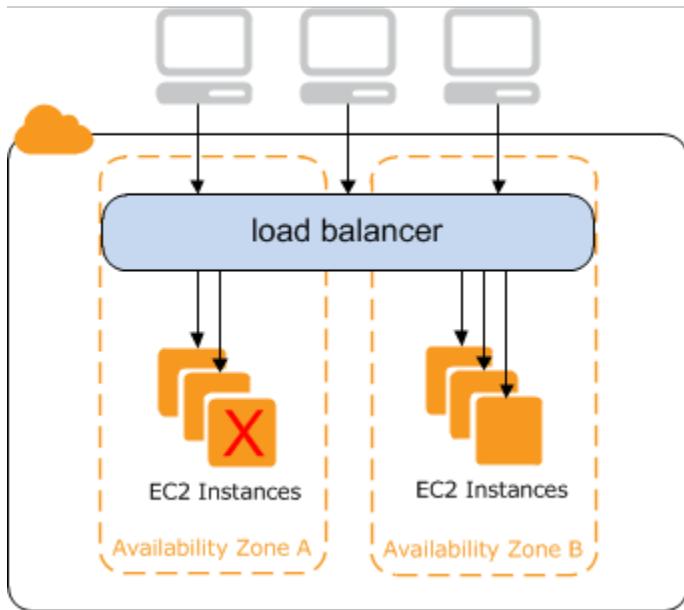
## Información general sobre equilibradores de carga clásicos

Un balanceador de carga distribuye el tráfico de aplicaciones entrante entre varias EC2 instancias en varias zonas de disponibilidad. Esto aumenta la tolerancia a errores de las aplicaciones. El ELB detecta las instancias en mal estado y dirige el tráfico solo a las instancias en buen estado.

El equilibrador de carga actúa como único punto de contacto para los clientes. Esto aumenta la disponibilidad de la aplicación. Puede agregar y eliminar instancias del equilibrador de carga de en función de sus necesidades sin interrumpir el flujo general de solicitudes a la aplicación. ELB escala el balanceador de carga a medida que el tráfico de la aplicación cambia con el tiempo. ELB puede adaptarse automáticamente a la gran mayoría de las cargas de trabajo.

Un oyente comprueba las solicitudes de conexión de los clientes mediante el protocolo y el puerto que haya configurado; a continuación, reenvía las solicitudes a una o más instancias registradas, utilizando el protocolo y el número de puerto que haya configurado. Puede agregar uno o varios oyentes al equilibrador de carga.

Puede configurar comprobaciones de estado, que se utilizan para supervisar el estado de las instancias registradas para que el equilibrador de carga envíe solo solicitudes a las instancias en buen estado.



Para asegurarse de que las instancias registradas puedan controlar la carga de solicitudes en cada zona de disponibilidad, es importante mantener aproximadamente el mismo número de instancias que están registradas en el equilibrador de carga en cada zona de disponibilidad. Por ejemplo, si tiene diez instancias en la zona de disponibilidad us-west-2a y dos en us-west-2b, las solicitudes se distribuyen de manera uniforme entre ambas zonas de disponibilidad. En consecuencia, las dos instancias de us-west-2b prestan servicio a la misma cantidad de tráfico que las diez instancias de us-west-2a. En lugar de ello, debería tener seis instancias en cada zona de disponibilidad.

De forma predeterminada, el equilibrador de carga distribuye equitativamente el tráfico entre las zonas de disponibilidad que se habilitan para el equilibrador de carga. Para distribuir el tráfico equitativamente entre todas las instancias registradas de todas las zonas de disponibilidad habilitadas, habilite el balanceo de carga entre zonas en el equilibrador de carga. Sin embargo, recomendamos mantener una cantidad aproximadamente equivalente de instancias en cada zona de disponibilidad para mejorar la tolerancia a errores.

Para obtener más información, consulta [Cómo funciona ELB](#) en la Guía del usuario de Elastic Load Balancing.

## Ventajas

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

- Compatibilidad con los oyentes TCP y SSL

- Compatibilidad con las sesiones persistentes mediante cookies generadas por la aplicación

Para obtener más información sobre las funciones compatibles con cada tipo de balanceador de carga, consulte [las comparaciones de productos del ELB](#).

## Cómo comenzar

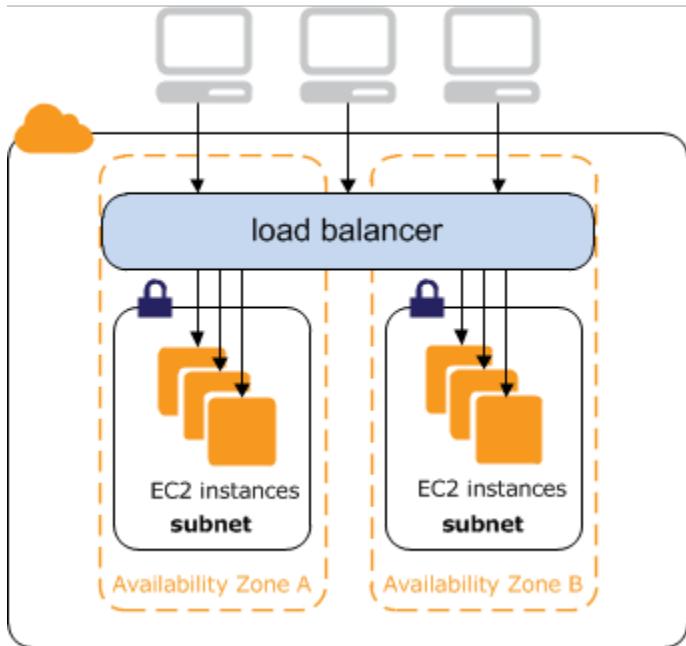
- Para obtener información sobre cómo crear un Classic Load Balancer y registrar EC2 instancias con él, consulte. [Creación de un Equilibrador de carga clásico expuesto a Internet](#)
- Para obtener información sobre cómo crear un balanceador de cargas HTTPS y registrar EC2 instancias con él, consulta. [Creación de un equilibrador de carga clásico con un oyente HTTPS](#)
- Para obtener información sobre cómo usar las distintas características que el Equilibrador de carga clásico admite, consulte [Configuración del equilibrador de carga clásico](#).

## Precios

Con el equilibrador de carga, solo se paga por lo que se usa. Para obtener más información, consulta los precios de [ELB](#).

# Equilibradores de carga clásicos expuestos a Internet

Al crear un Equilibrador de carga clásico, puede hacer que sea un equilibrador de carga interno o que esté expuesto a Internet. Un equilibrador de carga expuesto a Internet tiene un nombre de DNS que puede resolverse públicamente; por consiguiente, puede enrutar las solicitudes de los clientes a través de Internet a las instancias EC2 registradas en el equilibrador de carga.



El nombre de DNS de un equilibrador de carga interno se puede resolver para obtener las direcciones IP privadas de los nodos. Por lo tanto, los equilibradores de carga internos solo puede direccionar las solicitudes de los clientes que tienen acceso a la VPC para el equilibrador de carga. Para obtener más información, consulte [Equilibradores de carga internos](#).

## Contenido

- [Nombres de DNS públicos del equilibrador de carga](#)
- [Creación de un Equilibrador de carga clásico expuesto a Internet](#)

## Nombres de DNS públicos del equilibrador de carga

Al crear el equilibrador de carga, recibe un nombre de DNS público que los clientes pueden utilizar para enviar solicitudes. Los servidores DNS resuelven el nombre de DNS del equilibrador de carga para obtener las direcciones IP públicas de los nodos del equilibrador de carga. Cada nodo del equilibrador de carga está conectado a las instancias backend mediante direcciones IP privadas.

La consola muestra un nombre de DNS público con el siguiente formato:

`name-1234567890.region.elb.amazonaws.com`

## Creación de un Equilibrador de carga clásico expuesto a Internet

Al crear el equilibrador de carga, es preciso configurar los oyentes y las comprobaciones de estado, así como registrar las instancias backend. Para configurar un oyente, debe especificar un protocolo y un puerto para las conexiones frontend (del cliente al equilibrador de carga) y un protocolo y un puerto para las conexiones backend (del equilibrador de carga a las instancias backend). Puede configurar varios oyentes para el equilibrador de carga.

Este tutorial proporciona una introducción práctica a los balanceadores de carga clásicos a través de una interfaz basada en la web Consola de administración de AWS. Creará un balanceador de cargas que reciba tráfico HTTP público y lo envíe a sus instancias EC2.

Para crear un equilibrador de carga con un oyente HTTPS, consulte [Creación de un equilibrador de carga clásico con un oyente HTTPS](#).

### Tareas

- [Antes de empezar](#)
- [Cree un Classic Load Balancer con Consola de administración de AWS](#)

### Antes de empezar

- Cree una nube privada virtual (VPC). Para obtener más información, consulte [Recomendaciones para su VPC](#).
- Lanza las EC2 instancias que planeas registrar en tu balanceador de cargas. Asegúrese de que los grupos de seguridad de estas instancias permitan el acceso HTTP en el puerto 80.
- Instale un servidor web, por ejemplo, Apache o Internet Information Services (IIS), en cada instancia, escriba el nombre de DNS en el campo de direcciones de un navegador web conectado a Internet y compruebe que el navegador muestre la página predeterminada del servidor.

# Cree un Classic Load Balancer con Consola de administración de AWS

Siga el procedimiento a continuación para crear un equilibrador de carga. Proporcione información de configuración básica para el equilibrador de carga; por ejemplo, nombre y esquema. A continuación, proporcione información sobre la red y el oyente que dirige el tráfico hacia las instancias.

Para crear un Equilibrador de carga clásico 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 seleccionar la misma región que seleccionó para sus EC2 instancias.
3. En el panel de navegación, en Load Balancing (Equilibrio de carga), elija Load Balancers (Equilibradores de carga).
4. Elija Crear equilibrador de carga.
5. Amplíe la sección Equilibrador de carga clásico y, a continuación, seleccione Crear.
6. Configuración básica
  - a. En Nombre del equilibrador de carga, escriba un nombre para el equilibrador de carga.

El nombre del equilibrador de carga clásico debe ser único en el conjunto de equilibradores de carga clásicos de la región, puede tener un máximo de 32 caracteres, solo puede contener caracteres alfanuméricos y guiones y no puede comenzar ni finalizar con un guion.
  - b. En Esquema, seleccione Orientado a Internet.
7. Asignación de redes
  - a. En VPC, seleccione la misma VPC que haya seleccionado para las instancias.
  - b. En Asignaciones, primero seleccione una zona de disponibilidad, y luego una subred pública de las subredes disponibles de esta. Solo puede seleccionar una subred por cada zona de disponibilidad. Para mejorar la disponibilidad del equilibrador de carga, seleccione más de una zona de disponibilidad y subred.
8. Grupos de seguridad
  - En Grupos de seguridad, seleccione un grupo de seguridad existente que esté configurado para permitir el tráfico HTTP requerido en el puerto 80.
9. Los oyentes y el enrutamiento

- a. En Oyente, asegúrese de que el protocolo sea HTTP y el puerto 80.
- b. En Instancia, asegúrese de que el protocolo sea HTTP y el puerto 80.

#### 10. Comprobaciones de estado

- a. En Protocolo de ping, asegúrese de que el protocolo sea HTTP.
- b. En Puerto de ping, asegúrese de que el puerto sea 80.
- c. En Ruta de ping, asegúrese de que la ruta sea /.
- d. En Configuración avanzada de comprobación de estado, utilice los valores predeterminados.

#### 11. Instancias

- a. Seleccione Agregar instancias para que aparezca la pantalla de selección de instancias.
- b. En Instancias disponibles puede seleccionar entre las instancias actuales que estén disponibles para el equilibrador de carga, en función de la configuración de red actual.
- c. Cuando las selecciones le parezcan adecuadas, seleccione Confirmar para agregar las instancias que se deben registrar al equilibrador de carga.

#### 12. Atributos

- En Habilitar equilibrio de carga entre zonas, Habilitar drenaje de conexiones y Tiempo de espera (intervalo de drenaje), mantenga los valores predeterminados.

#### 13. Etiquetas del equilibrador de carga (opcionales)

- a. El campo Clave es obligatorio.
- b. El campo Valor es opcional.
- c. Para agregar otra etiqueta, seleccione Agregar nueva etiqueta y, a continuación, ingrese los valores en el campo Clave y, opcionalmente, en el campo Valor.
- d. Para eliminar una etiqueta existente, seleccione Eliminar junto a la etiqueta que desee eliminar.

#### 14. Resumen y creación

- a. Si necesita cambiar alguna configuración, seleccione Editar junto a la configuración que sea necesario modificar.

- b. Cuando todas las configuraciones mostradas en el resumen le parezcan adecuadas, seleccione Crear equilibrador de carga para comenzar con la creación del equilibrador de carga.
  - c. En la última página de creación, selecciona Ver balanceador de cargas para ver tu balanceador de cargas en la consola de Amazon EC2 .

#### 15. Verificar

- a. Seleccione el nuevo equilibrador de carga.
- b. En la pestaña Instancias de destino, compruebe la columna Estado. Cuando al menos una de tus EC2 instancias esté en servicio, puedes probar el balanceador de carga.
- c. En la sección Detalles, copie el Nombre de DNS del equilibrador de carga, que debe parecerse a `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`.
- d. Pegue el Nombre de DNS del equilibrador de carga en el campo de direcciones de un navegador web conectado a la Internet pública. Si el equilibrador de carga funciona correctamente, verá la página predeterminada del servidor.

#### 16. Eliminar (opcional)

- a. Si tiene un registro CNAME para el dominio que señala al equilibrador de carga, apúntelo hacia una nueva ubicación y espere a que surta efecto el cambio de DNS antes de eliminar el equilibrador de carga.
- b. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
- c. Seleccione el equilibrador de carga.
- d. Seleccione Acciones, Eliminar equilibrador de carga.
- e. Cuando se le pida confirmación, escriba `confirm` y seleccione Eliminar.
- f. Después de eliminar un balanceador de cargas, las EC2 instancias que se registraron en el balanceador de cargas seguirán ejecutándose. Se le facturará cada hora parcial o completa que sigan ejecutándose. Cuando ya no necesites una EC2 instancia, puedes detenerla o cancelarla para evitar incurrir en cargos adicionales.

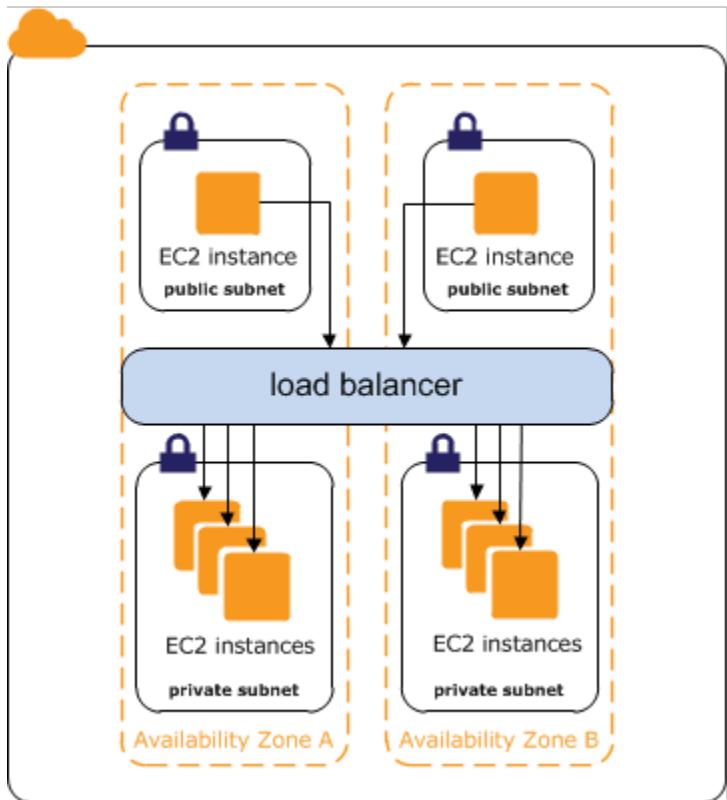
# Equilibradores de carga clásicos internos

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

Los nodos de un equilibrador de carga expuesto a internet tienen direcciones IP públicas. El nombre de DNS de un equilibrador de carga expuesto a internet se puede resolver públicamente para obtener las direcciones IP públicas de los nodos. Por tanto, los equilibradores de carga expuestos a internet pueden dirigir las solicitudes de los clientes a través de Internet. Para obtener más información, consulte [Equilibradores de carga clásicos expuestos a Internet](#).

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

Si la aplicación tiene varias capas (por ejemplo, servidores web que deben estar conectados a Internet y servidores de bases de datos que solo están conectados a los servidores web), puede diseñar una arquitectura que utilice equilibradores de carga internos y expuestos a Internet. Cree un equilibrador de carga expuesto a internet y registre los servidores web en él. Cree un equilibrador de carga interno y registre los servidores de bases de datos en él. Los servidores web reciben las solicitudes del equilibrador de carga expuesto a Internet y envían las solicitudes de los servidores de bases de datos al equilibrador de carga interno. Los servidores de bases de datos recibirán las solicitudes desde el equilibrador de carga interno.



## Contenido

- [Nombre DNS público del equilibrador de carga](#)
- [Creación de un Equilibrador de carga clásico interno](#)

## Nombre DNS público del equilibrador de carga

Cuando se crea un equilibrador de carga interno, recibe un nombre DNS público que tiene el formato siguiente:

`internal-name-123456789.region.elb.amazonaws.com`

Los servidores DNS resuelven el nombre DNS del equilibrador de carga en las direcciones IP privadas de los nodos del equilibrador de carga interno. Todos los nodos del equilibrador de carga están conectados a las direcciones IP privadas de las instancias backend a través de interfaces de red elásticas. Si el balanceo de carga está habilitado entre zonas, todos los nodos estarán conectados a cada una de las instancias backend, con independencia de la zona de disponibilidad. De lo contrario, cada nodo estará conectado únicamente a las instancias que se encuentren en su zona de disponibilidad.

# Creación de un Equilibrador de carga clásico interno

Puedes crear un balanceador de cargas interno para distribuir el tráfico a tus EC2 instancias desde los clientes con acceso a la VPC para el balanceador de cargas.

## Contenido

- [Requisitos previos](#)
- [Creación de un equilibrador de carga interno a través de la consola](#)
- [Crea un balanceador de cargas interno con el AWS CLI](#)

## Requisitos previos

- Si no ha creado una VPC para el equilibrador de carga, debe hacerlo antes de empezar. Para obtener más información, consulte [Recomendaciones para su VPC](#).
- Lanza las EC2 instancias que planeas registrar en tu balanceador de cargas interno. Asegúrese de que las lanza en las subredes privadas de la VPC que va a utilizar con el equilibrador de carga.

## Creación de un equilibrador de carga interno a través de la consola

Utilice el siguiente procedimiento para crear un Equilibrador de carga clásico interno. Proporcione información de configuración básica para el equilibrador de carga; por ejemplo, nombre y esquema. A continuación, proporcione información sobre la red y el oyente que dirige el tráfico hacia las instancias.

Para crear un Equilibrador de carga clásico interno 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 seleccionar la misma región que seleccionó para sus EC2 instancias.
3. En el panel de navegación, en Load Balancing (Equilibrio de carga), elija Load Balancers (Equilibradores de carga).
4. Elija Crear equilibrador de carga.
5. Amplíe la sección Equilibrador de carga clásico y, a continuación, seleccione Crear.
6. Configuración básica

- a. En Nombre del equilibrador de carga, escriba un nombre para el equilibrador de carga.

El nombre del equilibrador de carga clásico debe ser único en el conjunto de equilibradores de carga clásicos de la región, puede tener un máximo de 32 caracteres, solo puede contener caracteres alfanuméricos y guiones y no puede comenzar ni finalizar con un guion.

- a. En Esquema, seleccione Interno.

## 7. Asignación de redes

- a. En VPC, seleccione la misma VPC que haya seleccionado para las instancias.
- b. En Asignaciones, primero seleccione una zona de disponibilidad, y luego una subred de las subredes disponibles de esta. Solo puede seleccionar una subred por cada zona de disponibilidad. Para mejorar la disponibilidad del equilibrador de carga, seleccione más de una zona de disponibilidad y subred.

## 8. En Grupos de seguridad, seleccione un grupo de seguridad existente que esté configurado para permitir el tráfico HTTP requerido en el puerto 80. También puede crear un nuevo grupo de seguridad, en caso de que la aplicación utilice protocolos y puertos diferentes.

## 9. Los oyentes y el enrutamiento

- a. En Oyente, asegúrese de que el protocolo sea HTTP y el puerto 80.
- b. En Instancia, asegúrese de que el protocolo sea HTTP y el puerto 80.

## 10. Comprobaciones de estado

- a. Para Protocolo de ping, el valor predeterminado es HTTP.
- b. Para Puerto de ping, el valor predeterminado es 80.
- c. Para Ruta de ping, el valor predeterminado es /.
- d. En Configuración avanzada de comprobación de estado, utilice los valores predeterminados o introduzca valores específicos para su aplicación.

## 11. Instancias

- a. Seleccione Agregar instancias para que aparezca la pantalla de selección de instancias.
- b. En Instancias disponibles puede seleccionar entre las instancias actuales que estén disponibles para el equilibrador de carga, en función de la configuración de red seleccionada anteriormente.
- c. Cuando las selecciones le parezcan adecuadas, seleccione Confirmar para agregar las instancias que se deben registrar al equilibrador de carga.

## 12. Atributos

- En Habilitar equilibrio de carga entre zonas, Habilitar drenaje de conexiones y Tiempo de espera (intervalo de drenaje), mantenga los valores predeterminados.

## 13. Etiquetas del equilibrador de carga (opcionales)

- El campo Clave es obligatorio.
- El campo Valor es opcional.
- Para agregar otra etiqueta, seleccione Agregar nueva etiqueta y, a continuación, ingrese los valores en el campo Clave y, opcionalmente, en el campo Valor.
- Para eliminar una etiqueta existente, seleccione Eliminar junto a la etiqueta que deseé eliminar.

## 14. Resumen y creación

- Si necesita cambiar alguna configuración, seleccione Editar junto a la configuración que sea necesario modificar.
- Cuando todas las configuraciones mostradas en el resumen le parezcan adecuadas, seleccione Crear equilibrador de carga para comenzar con la creación del equilibrador de carga.
- En la última página de creación, selecciona Ver balanceador de cargas para ver tu balanceador de cargas en la consola de Amazon EC2 .

## 15. Verificar

- Seleccione el nuevo equilibrador de carga.
- En la pestaña Instancias de destino, compruebe la columna Estado. Cuando al menos una de tus EC2 instancias esté en servicio, puedes probar el balanceador de carga.
- En la sección Detalles, copie el Nombre de DNS del equilibrador de carga, que debe parecerse a `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`.
- Pegue el Nombre de DNS del equilibrador de carga en el campo de direcciones de un navegador web conectado a la Internet pública. Si el equilibrador de carga funciona correctamente, verá la página predeterminada del servidor.

## 16. Eliminar (opcional)

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

- b. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
- c. Seleccione el equilibrador de carga.
- d. Seleccione Acciones, Eliminar equilibrador de carga.
- e. Cuando se le pida confirmación, escriba **confirm** y seleccione Eliminar.
- f. Después de eliminar un balanceador de cargas, las EC2 instancias que se registraron en el balanceador de cargas seguirán ejecutándose. Se le facturará cada hora parcial o completa que sigan ejecutándose. Cuando ya no necesites una EC2 instancia, puedes detenerla o cancelarla para evitar incurrir en cargos adicionales.

## Crea un balanceador de cargas interno con el AWS CLI

De forma predeterminada, ELB crea un balanceador de cargas con conexión a Internet. Usa el siguiente procedimiento para crear un balanceador de cargas interno y registrar tus EC2 instancias con el balanceador de cargas interno recién creado.

Para crear un equilibrador de carga interno

1. Usa el [create-load-balancer](#) comando con la **--scheme** opción establecida en **internal**, de la siguiente manera:

```
aws elb create-load-balancer --load-balancer-name my-internal-loadbalancer --  
listeners Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80  
--subnets subnet-4e05f721 --scheme internal --security-groups sg-b9ffedd5
```

A continuación, se muestra un ejemplo de respuesta. Tenga en cuenta que el nombre indica que se trata de un equilibrador de carga interno.

```
{  
  "DNSName": "internal-my-internal-loadbalancer-786501203.us-  
west-2.elb.amazonaws.com"  
}
```

2. Usa el siguiente comando [register-instances-with-load-balancer](#) para añadir instancias:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-internal-  
loadbalancer --instances i-4f8cf126 i-0bb7ca62
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-4f8cf126"  
    },  
    {  
      "InstanceId": "i-0bb7ca62"  
    }  
  ]  
}
```

3. (Opcional) Usa el siguiente [describe-load-balancers](#) comando para verificar el balanceador de cargas interno:

```
aws elb describe-load-balancers --load-balancer-name my-internal-loadbalancer
```

La respuesta incluye los campos DNSName y Scheme, que indican que se trata de un equilibrador de carga interno.

```
{  
  "LoadBalancerDescriptions": [  
    {  
      ...  
      "DNSName": "internal-my-internal-loadbalancer-1234567890.us-  
      west-2.elb.amazonaws.com",  
      "SecurityGroups": [  
        "sg-b9ffedd5"  
      ],  
      "Policies": {  
        "LBCookieStickinessPolicies": [],  
        "AppCookieStickinessPolicies": [],  
        "OtherPolicies": []  
      },  
      "LoadBalancerName": "my-internal-loadbalancer",  
      "CreatedTime": "2014-05-22T20:32:19.920Z",  
      "AvailabilityZones": [  
        "us-west-2a"  
      ],  
      "Scheme": "internal",  
      "Type": "internal"  
    }  
  ]  
}
```

```
    ...  
    }  
]  
}
```

# Configuración del equilibrador de carga clásico

Después de crear un Equilibrador de carga clásico, puede cambiar su configuración. Por ejemplo, puede actualizar los atributos, las subredes y los grupos de seguridad del equilibrador de carga.

## Atributos del equilibrador de carga

### Drenaje de conexiones

Si está habilitado, el equilibrador de carga permite que las solicitudes existentes se completen antes de que el equilibrador de carga aparte el tráfico de una instancia anulada o con un estado incorrecto.

### Equilibrio de carga entre zonas

Si está habilitado, el equilibrador de carga dirige el tráfico de solicitudes de manera uniforme entre todas las instancias independientemente de las zonas de disponibilidad.

### Modo de mitigación de desincronización

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`.

### Tiempo de inactividad

Si está habilitado, el equilibrador de carga permite que las conexiones permanezcan inactivas (no se envían datos a través de la conexión) para la duración especificada. El valor predeterminado es de 60 segundos.

### Sesiones persistentes

Los Equilibradores de carga clásicos admiten una adherencia de sesión basada en la duración y basada en aplicaciones.

## Detalles del equilibrador de carga

### Grupos de seguridad

Los grupos de seguridad del equilibrador de carga deben permitir el tráfico entrante en los puertos de oyente y en los puertos de comprobación de estado.

## Subredes

Puede ampliar la disponibilidad del equilibrador de carga en subredes adicionales.

## Protocolo de proxy

Si está activado, añadimos un encabezado con la información de conexión que se envía a la instancia.

## Etiquetas

Puede agregar etiquetas para clasificar los equilibradores de carga.

# Configuración del tiempo de inactividad de conexión del equilibrador de carga clásico

Para cada solicitud que un cliente realiza a través de un equilibrador de carga clásico, el equilibrador de carga mantiene dos conexiones. La conexión front-end se realiza entre el cliente y el equilibrador de carga. La conexión de fondo es entre el balanceador de cargas y una instancia registrada. El equilibrador de carga tiene configurado un periodo de tiempo de espera de inactividad que se aplica a sus conexiones. Si no se han enviado ni recibido datos antes de que haya transcurrido el tiempo de inactividad, el equilibrador de carga cerrará 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.

Si utiliza oyentes HTTP y HTTPS, recomendamos habilitar la opción keep-alive de HTTP en las instancias. Puede habilitar keep-alive en los ajustes del servidor web para sus instancias. Cuando se habilita keep-alive, permite que el equilibrador de carga reutilice las conexiones back-end hasta que se agote el tiempo de espera de keep-alive. Para asegurarse de que el equilibrador de carga sea el responsable de cerrar las conexiones en la instancia, compruebe que el valor configurado para el tiempo de keep-alive de HTTP sea mayor que el tiempo de inactividad del equilibrador de carga.

Tenga en cuenta que las sondas keep-alive de TCP no impiden que el equilibrador de carga termine la conexión, ya que no envían datos en la carga útil.

## Contenido

- [Configuración del tiempo de inactividad desde la consola](#)

- [Configuración del tiempo de inactividad desde la AWS CLI](#)

## Configuración del tiempo de inactividad desde la consola

De forma predeterminada, ELB establece el tiempo de espera de inactividad del balanceador de carga en 60 segundos. Utilice el procedimiento siguiente para cambiar el tiempo de espera de inactividad.

Para configurar el tiempo de inactividad del 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 Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar atributos del equilibrador de carga, en la sección Configuración del tráfico, escriba un valor para Tiempo de espera de inactividad. El tiempo de inactividad debe estar comprendido entre 1 y 4,000 segundos.
6. Seleccione Save changes (Guardar cambios).

## Configuración del tiempo de inactividad desde la AWS CLI

Usa el siguiente [modify-load-balancer-attributes](#) comando para establecer el tiempo de espera de inactividad de tu balanceador de carga:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-Loadbalancer --load-balancer-attributes "{\"ConnectionSettings\":{\"IdleTimeout\":30}}"
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerAttributes": {  
    "ConnectionSettings": {  
      "IdleTimeout": 30  
    }  
  },  
  "LoadBalancerName": "my-loadbalancer"  
}
```

# Configuración del equilibrio de carga entre zonas en el equilibrador de carga clásico

Con el equilibrio de cargas entre zonas, cada nodo del equilibrador de carga de su equilibrador de carga clásico distribuye las solicitudes equitativamente entre todas las instancias registradas en todas las zonas de disponibilidad habilitadas. Si el equilibrio de cargas entre zonas está inhabilitado, cada nodo del equilibrador de carga distribuye las solicitudes equitativamente entre todas las instancias registradas solo en su zona de disponibilidad. Para obtener más información, consulte [Equilibrio de carga entre zonas](#) en la Guía del usuario de Elastic Load Balancing.

El balanceo de carga entre zonas reduce la necesidad de mantener un número equivalente de instancias en cada zona de disponibilidad habilitada y mejora la capacidad de la aplicación para controlar la pérdida de una o varias instancias. Sin embargo, recomendamos mantener una cantidad aproximadamente equivalente de instancias en cada zona de disponibilidad habilitada para aumentar la tolerancia a errores.

En los entornos donde los clientes almacenan en caché las búsquedas de DNS, las solicitudes entrantes podrían favorecer a una de las zonas de disponibilidad. Cuando se utiliza el equilibrio de carga entre zonas, este desequilibrio de la carga de solicitudes se distribuye entre todas las instancias disponibles de la región, por lo que se reduce el impacto de los clientes que se comportan de forma incorrecta.

Al crear un equilibrador de carga clásico, el valor predeterminado para el equilibrio de carga entre zonas depende de cómo se crea el equilibrador de carga. Con la API o el CLI, el equilibrio de carga entre zonas está deshabilitado de forma predeterminada. Con el Consola de administración de AWS, la opción de habilitar el equilibrio de carga entre zonas está seleccionada de forma predeterminada. Después de crear un equilibrador de carga clásico, puede habilitar o desactivar el equilibrio de carga entre zonas en cualquier momento.

## Contenido

- [Habilitación del equilibrio de carga entre zonas](#)
- [Desactivación del equilibrio de carga entre zonas](#)

## Habilitación del equilibrio de carga entre zonas

Puede habilitar el equilibrio de carga entre zonas del equilibrador de carga clásico en cualquier momento.

Para habilitar el balanceo 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 Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar atributos del equilibrador de carga, en la sección Configuración de enrutamiento de zonas de disponibilidad, habilite Equilibrio de carga entre zonas.
6. Seleccione Save changes (Guardar cambios).

Para habilitar el equilibrio de carga entre zonas, utilice el AWS CLI

1. Usa el siguiente [modify-load-balancer-attributes](#) comando para establecer el CrossZoneLoadBalancing atributo de tu balanceador de cargas en: true

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --  
load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":true}}"
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerAttributes": {  
    "CrossZoneLoadBalancing": {  
      "Enabled": true  
    }  
  },  
  "LoadBalancerName": "my-loadbalancer"  
}
```

2. (Opcional) Usa el siguiente [describe-load-balancer-attributes](#) comando para verificar que el balanceo de cargas entre zonas esté habilitado para tu balanceador de cargas:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerAttributes": {  
    "CrossZoneLoadBalancing": {  
      "Enabled": true  
    }  
  },  
  "LoadBalancerName": "my-loadbalancer",  
  "Scheme": "internet-facing",  
  "Subnets": [  
    "subnet-00000000",  
    "subnet-00000001",  
    "subnet-00000002",  
    "subnet-00000003"  
  ],  
  "Type": "classic",  
  "VPCId": "vpc-00000000",  
  "ZoneId": "us-east-1a",  
  "HealthCheck": {  
    "HealthCheckInterval": 50, "HealthyThreshold": 3, "UnhealthyThreshold": 2, "Timeout": 5, "Type": "HTTP", "URI": "/"}  
}
```

```
        "ConnectionDraining": {  
            "Enabled": false,  
            "Timeout": 300  
        },  
        "CrossZoneLoadBalancing": {  
            "Enabled": true  
        },  
        "ConnectionSettings": {  
            "IdleTimeout": 60  
        },  
        "AccessLog": {  
            "Enabled": false  
        }  
    }  
}
```

## Desactivación del equilibrio de carga entre zonas

Puede deshabilitar la opción de balanceo de carga entre zonas del equilibrador de carga en cualquier momento.

Para deshabilitar el balanceo 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 Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar atributos del equilibrador de carga, en la sección Configuración de enrutamiento de zonas de disponibilidad, deshabilite Equilibrio de carga entre zonas.
6. Seleccione Save changes (Guardar cambios).

Para deshabilitar el balanceo de carga entre zonas, defina el atributo `CrossZoneLoadBalancing` del equilibrador de carga en `false`.

Para deshabilitar el balanceo de carga entre zonas, utilice el AWS CLI

1. Utilice el siguiente comando [`modify-load-balancer-attributes`](#):

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --  
load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":false}}"
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerAttributes": {  
    "CrossZoneLoadBalancing": {  
      "Enabled": false  
    }  
  },  
  "LoadBalancerName": "my-loadbalancer"  
}
```

2. (Opcional) Usa el siguiente [describe-load-balancer-attributes](#) comando para verificar que el equilibrio de cargas entre zonas esté desactivado para tu balanceador de cargas:

```
aws elb describe-load-balancer-attributes --load-balancer-name my-Loadbalancer
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerAttributes": {  
    "ConnectionDraining": {  
      "Enabled": false,  
      "Timeout": 300  
    },  
    "CrossZoneLoadBalancing": {  
      "Enabled": false  
    },  
    "ConnectionSettings": {  
      "IdleTimeout": 60  
    },  
    "AccessLog": {  
      "Enabled": false  
    }  
  }  
}
```

# Configuración de drenaje de conexiones en el equilibrador de carga clásico

Para asegurarse de que el equilibrador de carga clásico deje de enviar solicitudes a las instancias que están en proceso de anulación del registro o se encuentran en mal estado, pero mantener abiertas las conexiones existentes, utilice drenaje de conexiones. De este modo, se permite que el equilibrador de carga complete las solicitudes en tránsito a las instancias que están en proceso de anulación del registro o se encuentran en mal estado.

Al habilitar el drenaje de conexiones puede especificar el tiempo máximo durante el cual el equilibrador de carga mantendrá activas las conexiones antes de considerar que se ha anulado el registro de la instancia. El tiempo de espera máximo puede establecerse entre 1 y 3600 segundos (el valor predeterminado es de 300 segundos). Cuando ha transcurrido el plazo máximo, el equilibrador de carga cierra forzosamente las conexiones para anular el registro de la instancia.

Si una instancia que se cancela del registro no tiene solicitudes en curso ni conexiones activas, ELB completa inmediatamente el proceso de anulación del registro.

Mientras se están atendiendo las solicitudes en tránsito, el equilibrador de carga notifica que el estado de la instancia es `InService: Instance deregistration currently in progress`. Una vez que la instancia en proceso de anulación del registro ha terminado de atender a todas las solicitudes en tránsito, o cuando se ha agotado el tiempo de espera máximo, el equilibrador de carga notifica que el estado de la instancia es `OutOfService: Instance is not currently registered with the LoadBalancer`.

Si una instancia pasa a encontrarse en mal estado, el equilibrador de carga notifica que el estado de la instancia es `OutOfService`. Si hay solicitudes en tránsito que se han realizado a la instancia en mal estado, se completan. El tiempo de espera máximo no se aplica a las conexiones con instancias en mal estado.

Si las instancias forman parte de un grupo de escalado automático y se habilita drenaje de conexiones en el equilibrador de carga, El escalado automático espera que se completen las solicitudes en tránsito o que se agote el tiempo de espera máximo antes de terminar las instancias debido a un evento de escalado o a una sustitución por comprobación de estado.

Puede deshabilitar el drenaje de conexiones si desea que el equilibrador de carga cierre de inmediato las conexiones a las instancias que están en proceso de anulación del registro o se encuentran en mal estado. Cuando el drenaje de conexiones está deshabilitado, no se completan

las solicitudes en tránsito realizadas a instancias que están en proceso de anulación del registro o se encuentran en mal estado.

## Contenido

- [Habilitación del drenaje de conexiones](#)
- [Desactivación de drenaje de conexiones](#)

## Habilitación del drenaje de conexiones

Puede habilitar el drenaje de conexiones del equilibrador de carga en cualquier momento.

Para habilitar el drenaje de conexiones 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 para abrir su página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar atributos del equilibrador de carga, en la sección Configuración del tráfico, seleccione Habilitar drenaje de conexiones.
6. (Opcional) En Tiempo de espera (intervalo de drenaje), escriba un valor comprendido entre 1 y 3600 segundos. De lo contrario, se aplicarán 300 segundos, el valor predeterminado.
7. Seleccione Save changes (Guardar cambios).

Para habilitar el agotamiento de la conexión mediante el AWS CLI

Utilice el siguiente comando [modify-load-balancer-attributes](#):

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":true,\"Timeout\":300}}"
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerAttributes": {  
    "ConnectionDraining": {  
      "Enabled": true,  
      "Timeout": 300  
    }  
  }  
}
```

```
        "Timeout": 300
    }
},
"LoadBalancerName": "my-loadbalancer"
}
```

## Desactivación de drenaje de conexiones

Puede deshabilitar el drenaje de conexiones del equilibrador de carga en cualquier momento.

Para deshabilitar el drenaje de conexiones 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 para abrir su página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar atributos del equilibrador de carga, en la sección Configuración del tráfico, anule la selección de Habilitar drenaje de conexiones.
6. Seleccione Save changes (Guardar cambios).

Para deshabilitar el agotamiento de la conexión mediante el AWS CLI

Utilice el siguiente comando [modify-load-balancer-attributes](#):

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":false}}"
```

A continuación, se muestra un ejemplo de respuesta:

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

# Configuración de sesiones persistentes para el Equilibrador de carga clásico

De forma predeterminada, un equilibrador de carga clásico enruta cada solicitud de manera independiente a la instancia registrada con menor carga. 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 a la misma instancia.

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 su aplicación tiene su propia cookie de sesión, puede configurar ELB para que la cookie de sesión tenga la duración especificada por la cookie de sesión de la aplicación. Si su aplicación no tiene su propia cookie de sesión, puede configurar ELB para que cree una cookie de sesión especificando su propia duración de permanencia.

ELB crea una cookie, denominada AWSELB, que se utiliza para asignar la sesión a la instancia.

## Requisitos

- Un HTTP/HTTPS balanceador de cargas.
- Al menos una instancia en buen estado en cada zona de disponibilidad.

## Compatibilidad

- El RFC de la propiedad de ruta de una cookie admite los guiones bajos. Sin embargo, el URI del ELB codifica los caracteres de subrayado %5F porque algunos navegadores, como Internet Explorer 7, esperan que los guiones bajos estén codificados como URI. %5F Debido a la posibilidad de afectar a los navegadores que funcionan actualmente, el ELB sigue codificando los caracteres de subrayado en el URI. Por ejemplo, si la cookie tiene la propiedad `path=/my_path`, ELB cambia esta propiedad en la solicitud reenviada a `path=/my%5Fpath`
- No se pueden establecer las marcas `secure` ni `HttpOnly` en las cookies de las sesiones persistentes basadas en duración. Sin embargo, estas cookies no contienen información confidencial. Tenga en cuenta que si establece el `secure` indicador o el `HttpOnly` indicador en una cookie de persistencia de sesión controlada por la aplicación, también se configurará en la cookie. AWSELB

- Si hay un signo de punto y coma final en el campo Set-Cookie de una cookie de aplicación, el equilibrador de carga hace caso omiso de la cookie.

## Contenido

- [Persistencia de las sesiones en función de la duración](#)
- [Persistencia de las sesiones controlada por la aplicación](#)

## Persistencia de las sesiones en función de la duración

El balanceador de cargas usa una cookie especial, AWSELB, para rastrear la instancia de cada solicitud dirigida a cada oyente. Cuando el equilibrador de carga recibe una solicitud, primero comprueba si esta cookie está presente en la solicitud. En caso afirmativo, la solicitud se envía a la instancia especificada en la cookie. Si no hay ninguna cookie, el equilibrador de carga elige una instancia en función del algoritmo de balanceo de carga existente. Se inserta una cookie en la respuesta para vincular las solicitudes posteriores del mismo usuario a esa instancia. La configuración de la política de persistencia define el vencimiento de la cookie, que establece el periodo de validez de cada cookie. El equilibrador de carga no actualiza el tiempo de caducidad de la cookie ni comprueba si ha caducado antes de usarla. Una vez que la cookie ha vencido, la sesión ya no es persistente. El cliente debe quitar la cookie de su almacén de cookies una vez caducada.

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

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 instancia en buen estado en función del algoritmo de equilibrio de carga existente. La solicitud se redirecciona a la nueva instancia como si no hubiera ninguna cookie y la sesión deja de ser persistente.

Si un cliente cambia a un oyente con un puerto backend diferente, la persistencia se pierde.

Para habilitar las sesiones persistentes basadas en duración en 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, en Equilibrio de carga, elija Equilibradores de carga.

3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Oyentes, seleccione Administrar oyentes.
5. En la página Administrar oyentes, localice el oyente que desea actualizar y seleccione Editar en Persistencia de cookie.
6. En la ventana emergente Editar la configuración de persistencia de las cookies, seleccione Generado por el equilibrador de cargas.
7. (Opcional) En Periodo de vencimiento, escriba el periodo de vencimiento de la cookie en segundos. Si no especifica un periodo de vencimiento, la sesión persistente durará lo mismo que la sesión del navegador.
8. Seleccione Guardar cambios para cerrar la ventana.
9. Seleccione Guardar cambios para volver a la página de detalles del equilibrador de carga.

Para habilitar las sesiones persistentes basadas en duración en un equilibrador de carga desde la AWS CLI

1. Usa el siguiente comando [`create-lb-cookie-stickiness-policy`](#) para crear una política de adherencia de cookies generada por un balanceador de carga con un período de caducidad de 60 segundos:

```
aws elb create-lb-cookie-stickiness-policy --load-balancer-name my-loadbalancer --policy-name my-duration-cookie-policy --cookie-expiration-period 60
```

2. Usa el siguiente comando [`set-load-balancer-policies-of-listener`](#) para habilitar la adherencia de la sesión en el balanceador de cargas especificado:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --load-balancer-port 443 --policy-names my-duration-cookie-policy
```

 Note

El comando `set-load-balancer-policies-of-listener` reemplaza el conjunto actual de políticas asociadas con el puerto del equilibrador de carga especificado. Cada vez que se utiliza el comando, debe especificar la opción `--policy-names` para enumerar todas las políticas que hay que habilitar.

3. (Opcional) Usa el siguiente [describe-load-balancers](#) comando para comprobar que la política esté habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La respuesta incluye la siguiente información, que muestra que la política está habilitada para el oyente en el puerto especificado:

```
{  
    "LoadBalancerDescriptions": [  
        {  
            ...  
            "ListenerDescriptions": [  
                {  
                    "Listener": {  
                        "InstancePort": 443,  
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-  
certificate/my-server-certificate",  
                        "LoadBalancerPort": 443,  
                        "Protocol": "HTTPS",  
                        "InstanceProtocol": "HTTPS"  
                    },  
                    "PolicyNames": [  
                        "my-duration-cookie-policy",  
                        "ELBSecurityPolicy-TLS-1-2-2017-01"  
                    ]  
                },  
                ...  
            ],  
            ...  
            "Policies": {  
                "LBCookieStickinessPolicies": [  
                    {  
                        "PolicyName": "my-duration-cookie-policy",  
                        "CookieExpirationPeriod": 60  
                    }  
                ],  
                "AppCookieStickinessPolicies": [],  
                "OtherPolicies": [  
                    "ELBSecurityPolicy-TLS-1-2-2017-01"  
                ]  
            }  
        }  
    ]  
}
```

```
    },
    ...
}
]
```

## Persistencia de las sesiones controlada por la aplicación

El equilibrador de carga utiliza una cookie especial para asociar la sesión con la instancia que controló la solicitud inicial, pero respeta la vida útil de la cookie de aplicación especificada en la configuración de la política. El equilibrador de carga solo inserta una nueva cookie de persistencia si la respuesta de la aplicación incluye una nueva cookie de aplicación. La cookie de persistencia del equilibrador de carga no se actualiza con cada solicitud. Si la cookie de aplicación se elimina de forma explícita o vence, la sesión deja de ser persistente hasta que se emite una nueva cookie de aplicación.

Los siguientes atributos establecidos por instancias backend se envían a los clientes en la cookie: `path`, `port`, `domain`, `secure`, `httponly`, `discard`, `max-age`, `expires`, `version`, `comment`, `commenturl` y `samesite`.

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 instancia en buen estado en función del algoritmo de equilibrio de carga existente. El equilibrador de carga trata la sesión como si estuviera "pegada" 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.

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 Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Oyentes, seleccione Administrar oyentes.
5. En la página Administrar oyentes, localice el oyente que desea actualizar y seleccione Editar en Persistencia de cookie.
6. Seleccione Generada por la aplicación.
7. En Cookie name (Nombre de cookie), escriba el nombre de la cookie de la aplicación.
8. Seleccione Save changes (Guardar cambios).

Para habilitar la persistencia de las sesiones controlada por la aplicación mediante el AWS CLI

1. Utilice el siguiente comando `create-app-cookie-stickiness-policy` para crear una política de adherencia de las cookies generada por la aplicación:

```
aws elb create-app-cookie-stickiness-policy --load-balancer-name my-loadbalancer --policy-name my-app-cookie-policy --cookie-name my-app-cookie
```

2. Usa el siguiente comando [set-load-balancer-policies-of-listener](#) para habilitar la adherencia de la sesión en un balanceador de cargas:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --load-balancer-port 443 --policy-names my-app-cookie-policy
```

 Note

El comando `set-load-balancer-policies-of-listener` reemplaza el conjunto actual de políticas asociadas con el puerto del equilibrador de carga especificado.

Cada vez que se utiliza el comando, debe especificar la opción `--policy-names` para enumerar todas las políticas que hay que habilitar.

3. (Opcional) Usa el siguiente [describe-load-balancers](#) comando para comprobar que la política fija esté habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

4. La respuesta incluye la siguiente información, que muestra que la política está habilitada para el oyente en el puerto especificado:

```
{  
  "LoadBalancerDescriptions": [  
    {  
      ...  
      "ListenerDescriptions": [  
        {  
          "Listener": {  
            "InstancePort": 443,  
            "SSLCertificateId": "arn:aws:iam::123456789012:server-  
certificate/my-server-certificate",  
            "LoadBalancerPort": 443,  
            "Protocol": "TLS",  
            "SslCertificate": {  
              "Arn": "arn:aws:iam::123456789012:server-  
certificate/my-server-certificate",  
              "Id": "arn:aws:iam::123456789012:server-  
certificate/my-server-certificate",  
              "Name": "my-server-certificate",  
              "Type": "Server",  
              "ValidFrom": "2023-01-01T00:00:00Z",  
              "ValidUntil": "2024-01-01T00:00:00Z",  
              "Subject": "CN=*.myserver.com",  
              "SubjectAltNames": ["*.myserver.com"],  
              "SubjectKeyIdentifier": "...',  
              "Thumbprint": "...",  
              "ThumbprintSha256": "...",  
              "Version": 1  
            }  
          }  
        }  
      ]  
    }  
  ]  
}
```

```
        "Protocol": "HTTPS",
        "InstanceProtocol": "HTTPS"
    },
    "PolicyNames": [
        "my-app-cookie-policy",
        "ELBSecurityPolicy-TLS-1-2-2017-01"
    ]
},
{
    "Listener": {
        "InstancePort": 80,
        "LoadBalancerPort": 80,
        "Protocol": "TCP",
        "InstanceProtocol": "TCP"
    },
    "PolicyNames": []
}
],
...
"Policies": {
    "LBCookieStickinessPolicies": [],
    "AppCookieStickinessPolicies": [
    {
        "PolicyName": "my-app-cookie-policy",
        "CookieName": "my-app-cookie"
    }
    ],
    "OtherPolicies": [
        "ELBSecurityPolicy-TLS-1-2-2017-01"
    ]
},
...
}
]
```

# Configuración de modo de mitigación de desincronización del equilibrador de carga clásico

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.

## Contenido

- [Clasificaciones](#)
- [Modos](#)
- [Modificación del modo de mitigación de desincronización](#)

### Tip

Esta configuración solo se aplica a los equilibradores de carga clásicos. Para obtener información que se aplique a los equilibradores de carga de aplicaciones, consulte [Modo de mitigación de desincronización para equilibradores de carga de aplicaciones](#).

## 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.

En las listas que se incluyen a continuación, se describen los problemas correspondientes a cada clasificación.

#### Aceptable

- Un encabezado contiene un carácter de control o no ASCII.
- La versión de la solicitud contiene un valor incorrecto.
- Hay un encabezado Content-Length con un valor de 0 para una solicitud GET o HEAD.
- El URI de la solicitud contiene un espacio sin codificación URL.

#### Ambigua

- El URI de la solicitud contiene caracteres de control.
- La solicitud contiene un encabezado Transfer-Encoding y un encabezado Content-Length.
- Hay varios encabezados Content-Length con el mismo valor.
- Un encabezado está vacío o hay una línea que solo contiene espacios.
- Hay un encabezado que se puede normalizar a Transfer-Encoding o Content-Length mediante técnicas comunes de normalización de texto.
- Hay un encabezado Content-Length para una solicitud GET o HEAD.
- Hay un encabezado Transfer-Encoding para una solicitud GET o HEAD.

#### Grave

- El URI de la solicitud contiene un carácter nulo o un retorno de carro.
- El encabezado Content-Length contiene un valor que no se puede analizar o que no es un número válido.
- Un encabezado contiene un carácter nulo o un retorno de carro.
- El encabezado Transfer-Encoding contiene un valor incorrecto.
- El método de la solicitud tiene un formato incorrecto.
- La versión de la solicitud tiene un formato incorrecto.
- Hay varios encabezados Content-Length con valores diferentes.

- Hay varios encabezados Transfer-Encoding fragmentados.

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 clásico](#).

## Modos

En la siguiente tabla se describe cómo los equilibradores de carga clásicos 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 <sup>1</sup>	Bloqueada
Grave	Permitido	Bloqueada	Bloqueada

<sup>1</sup> Enruta las solicitudes, pero cierra las conexiones del cliente y del destino.

## Modificación del modo de mitigación de desincronización

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, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar atributos del equilibrador de carga, en Configuración del tráfico, seleccione Defensiva (recomendado), La más estricta o Monitorear.
6. Seleccione Save changes (Guardar cambios).

Para actualizar el modo de mitigación desincronizado mediante el AWS CLI

Utilice el [modify-load-balancer-attributes](#) comando con el `elb.http.desyncmitigationmode` atributo establecido en `monitordefensive`, o `strictest`

```
aws elb modify-load-balancer-attributes --load-balancer-name my-load-balancer --load-balancer-attributes file://attribute.json
```

A continuación, se muestra el contenido de `attribute.json`.

```
{  
  "AdditionalAttributes": [  
    {  
      "Key": "elb.http.desyncmitigationmode",  
      "Value": "strictest"  
    }  
  ]  
}
```

## Configuración del protocolo de proxy del Equilibrador de carga clásico

Proxy Protocol es un protocolo de Internet que se utiliza para transportar la información de conexión entre el origen que solicita la conexión y el destino al cual se solicita dicha conexión. ELB usa la versión 1 del protocolo proxy, que usa un formato de encabezado legible por humanos.

De forma predeterminada, cuando se utiliza el protocolo de control de transmisión (TCP) para las conexiones frontend y backend, el equilibrador de carga clásico reenvía las solicitudes a las instancias sin modificar sus encabezados. Si habilita Proxy Protocol, se agrega un encabezado en formato de lenguaje natural al encabezado de la solicitud. Este contiene información de la conexión como, por ejemplo, las direcciones IP de origen y destino, y los números de puerto. A continuación, el encabezado se envía a la instancia como parte de la solicitud.

### Note

No Consola de administración de AWS admite la activación del protocolo proxy.

## Contenido

- [Encabezado Proxy Protocol](#)

- [Requisitos previos para habilitar Proxy Protocol](#)
- [Habilitación de Proxy Protocol desde la AWS CLI](#)
- [Desactivación de Proxy Protocol desde la AWS CLI](#)

## Encabezado Proxy Protocol

El encabezado Proxy Protocol ayuda a identificar la dirección IP de un cliente cuando el equilibrador de carga utiliza TCP para las conexiones backend. Dado que los equilibradores de carga interceptan el tráfico entre los clientes y las instancias, los registros de acceso desde la instancia contienen la dirección IP del equilibrador de carga, y no la del cliente de origen. Puede analizar la primera línea de la solicitud para recuperar la dirección IP del cliente y el número de puerto.

La dirección del proxy que aparece en el encabezado IPv6 es la IPv6 dirección pública de tu balanceador de cargas. Esta IPv6 dirección coincide con la dirección IP que se resuelve a partir del nombre DNS del balanceador de cargas, que comienza por `oipv6.dualstack`. Si el cliente se conecta con IPv4, la dirección del proxy del encabezado es la IPv4 dirección privada del equilibrador de cargas, que no se puede resolver mediante una búsqueda de DNS.

La línea de Proxy Protocol es una sola línea que termina con un retorno de carro y un salto de línea ("`\r\n`"). Presenta el siguiente formato:

```
PROXY_STRING + single space + INET_PROTOCOL + single space + CLIENT_IP + single space +  
PROXY_IP + single space + CLIENT_PORT + single space + PROXY_PORT + "\r\n"
```

Ejemplo: IPv4

A continuación se muestra un ejemplo de la línea de protocolo proxy para IPv4

```
PROXY TCP4 198.51.100.22 203.0.113.7 35646 80\r\n
```

## Requisitos previos para habilitar Proxy Protocol

Antes de comenzar, haga lo siguiente:

- Confirme que el equilibrador de carga no se encuentre tras un servidor proxy con Proxy Protocol habilitado. Si Proxy Protocol está habilitado en el servidor proxy y también en el equilibrador de carga, este último agregará un encabezado más a la solicitud, que ya tiene un encabezado del

servidor proxy. Según cómo esté configurada la instancia, esta duplicación podría dar lugar a errores.

- Confirme que las instancias puedan procesar la información de Proxy Protocol.
- Confirme que la configuración del oyente admita Proxy Protocol. Para obtener más información, consulte [Configuraciones de oyentes para los equilibradores de carga clásicos](#).

## Habilitación de Proxy Protocol desde la AWS CLI

Para habilitar Proxy Protocol, se debe crear una política de tipo `ProxyProtocolPolicyType` y, a continuación, habilitar la política en el puerto de la instancia.

Utilice el siguiente procedimiento para crear una nueva política del tipo `ProxyProtocolPolicyType` para el equilibrador de carga, establecer la política recién creada para la instancia en el puerto 80 y comprobar que la política está habilitada.

Para habilitar Proxy Protocol en el equilibrador de carga

1. (Opcional) Utilice el siguiente comando [describe-load-balancer-policy-types](#) para enumerar las políticas compatibles con ELB:

```
aws elb describe-load-balancer-policy-types
```

La respuesta incluye los nombres y las descripciones de los tipos de políticas admitidos. A continuación se muestra el resultado para el tipo `ProxyProtocolPolicyType`:

```
{  
  "PolicyTypeDescriptions": [  
    ...  
    {  
      "PolicyAttributeTypeDescriptions": [  
        {  
          "Cardinality": "ONE",  
          "AttributeName": "ProxyProtocol",  
          "AttributeType": "Boolean"  
        }  
      ],  
      "PolicyTypeName": "ProxyProtocolPolicyType",  
      "Description": "Policy that controls whether to include the IP address  
      and port of the originating
```

```
request for TCP messages. This policy operates on TCP/SSL listeners only"
    },
    ...
]
}
```

2. Use el siguiente [create-load-balancer-policy](#) comando para crear una política que habilite el protocolo proxy:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-name my-ProxyProtocol-policy --policy-type-name ProxyProtocolPolicyType --policy-attributes AttributeName=ProxyProtocol,AttributeValue=true
```

3. Use el siguiente [set-load-balancer-policies-](#) comando para habilitar la política recién creada en el puerto especificado. Tenga en cuenta que este comando sustituye el conjunto actual de políticas habilitadas. Por lo tanto, la opción --policy-names debe especificar tanto la política que se va a agregar a la lista (por ejemplo, my-ProxyProtocol-policy) como todas las políticas que ya estén habilitadas (por ejemplo, my-existing-policy).

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-ProxyProtocol-policy my-existing-policy
```

4. (Opcional) Utilice el siguiente [describe-load-balancers](#) comando para comprobar que el protocolo proxy esté habilitado:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La respuesta incluye la siguiente información, que muestra que la política my-ProxyProtocol-policy está asociada al puerto 80.

```
{
  "LoadBalancerDescriptions": [
    {
      ...
      "BackendServerDescriptions": [
        {
          "InstancePort": 80,
          "PolicyNames": [
            "my-ProxyProtocol-policy"
          ]
        }
      ]
    }
  ]
}
```

```
        ]
      ],
      ...
    ]
}
```

## Desactivación de Proxy Protocol desde la AWS CLI

Puede deshabilitar las políticas asociadas a la instancia y habilitarlas más adelante.

Para desactivar la política de Proxy Protocol

1. Use el siguiente for-backend-server comando [set-load-balancer-policies](#): para deshabilitar la política de protocolo proxy omitiéndola de la --policy-names opción, pero incluyendo las demás políticas que deberían permanecer habilitadas (por ejemplo, *my-existing-policy*).

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-existing-policy
```

Si no hay otras políticas que habilitar, especifique una cadena vacía con la opción --policy-names, de la siguiente manera:

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names "[]"
```

2. (Opcional) Utilice el siguiente [describe-load-balancers](#) comando para comprobar que la política está deshabilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La respuesta incluye la siguiente información, que muestra que no hay ningún puerto asociado a una política.

```
{
  "LoadBalancerDescriptions": [
    {
      ...
    }
  ]
}
```

```
        "BackendServerDescriptions": [],
        ...
    }
}
```

## Etiquetado del equilibrador de carga clásico

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 clásico. Las claves de las etiquetas deben ser únicas en 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.

### Contenido

- [Restricciones de las etiquetas](#)
- [Añada una etiqueta](#)
- [Eliminación de una etiqueta](#)

### Restricciones de las etiquetas

Se aplican las siguientes restricciones básicas a las etiquetas de :

- 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.

## Añada una etiqueta

Puede agregar etiquetas al equilibrador de carga en cualquier momento.

Para agregar una etiqueta 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 para abrir su página de detalles.
4. En la pestaña Etiquetas, elija Administrar etiquetas.
5. En la página Administrar etiquetas, seleccione Agregar nueva etiqueta para cada etiqueta y, a continuación, especifique una clave y un valor.
6. Cuando haya terminado de agregar etiquetas, seleccione Guardar cambios.

Para añadir una etiqueta mediante el AWS CLI

Utilice el siguiente comando [add-tags](#) para agregar la etiqueta especificada:

```
aws elb add-tags --load-balancer-name my-loadbalancer --tag "Key=project,Value=Lima"
```

## Eliminación de una etiqueta

Puede eliminar etiquetas del equilibrador de carga en cualquier momento si ha terminado de utilizarlas.

Para eliminar una etiqueta 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 para abrir su página de detalles.
4. En la pestaña Etiquetas, elija Administrar etiquetas.
5. En la página Administrar etiquetas, seleccione Eliminar junto a cada etiqueta que desee quitar.
6. Cuando haya terminado de eliminar etiquetas, seleccione Guardar cambios.

Para quitar una etiqueta utilizando el AWS CLI

Utilice el siguiente comando [remove-tags](#) para eliminar la etiqueta que tiene la clave especificada:

```
aws elb remove-tags --load-balancer-name my-Loadbalancer --tag project
```

## Configuración de subredes del Equilibrador de carga clásico

Cuando agregas una subred a tu balanceador de cargas, ELB crea un nodo balanceador de cargas en la zona de disponibilidad. Los nodos de equilibrador de carga aceptan el tráfico procedente de los clientes y reenvían solicitudes a las instancias en buen estado registradas en una o varias zonas de disponibilidad. Le recomendamos que agregue una subred por cada zona de disponibilidad en al menos dos zonas de disponibilidad. De este modo, mejora la disponibilidad del equilibrador de carga. Tenga en cuenta que las subredes del equilibrador de carga pueden modificarse en cualquier momento.

Seleccione subredes de las mismas zonas de disponibilidad como instancias. Si el equilibrador de carga está expuesto a Internet, debe seleccionar subredes públicas para que sus instancias backend puedan recibir el tráfico procedente del equilibrador de carga (incluso si las instancias backend se encuentran en subredes privadas). Si el equilibrador de carga es interno, le recomendamos que seleccione subredes privadas. Para obtener más información sobre las subredes del equilibrador de carga, consulte [Recomendaciones para su VPC](#).

Para añadir una subred, registre las instancias en la Zona de disponibilidad con el equilibrador de carga y, a continuación, asocie una subred de la zona de disponibilidad al equilibrador de carga. Para obtener más información, consulte [Registrar instancias con el Equilibrador de carga clásico](#).

Después de agregar una subred, el equilibrador de carga comienza a direccionar solicitudes a las instancias registradas en la zona de disponibilidad correspondiente. De forma predeterminada, el equilibrador de carga dirige las solicitudes de forma uniforme a través de las zonas de disponibilidad de sus subredes. Para dirigir las solicitudes de forma uniforme entre todas las instancias registradas en las zonas de disponibilidad de sus subredes, habilite el balanceo de carga entre zonas. Para obtener más información, consulte [Configuración del equilibrio de carga entre zonas en el equilibrador de carga clásico](#).

Es posible que quiera eliminar temporalmente una subred del equilibrador de carga porque ninguna de las instancias registradas en la zona de disponibilidad tenga un estado correcto, porque deba solucionar problemas con las instancias registradas o porque necesite actualizarlas. Después de eliminar una subred, el equilibrador de carga deja de dirigir las solicitudes a las instancias registradas en su zona de disponibilidad, aunque sigue dirigiéndolas a las instancias registradas

de las zonas de disponibilidad de las subredes restantes. Tenga en cuenta que, después de eliminar una subred, las instancias de esa subred siguen registradas con el equilibrador de carga, pero puede anular el registro si así lo desea. Para obtener más información, consulte [Registrar instancias con el Equilibrador de carga clásico](#).

## Contenido

- [Requisitos](#)
- [Configurar las subredes con la consola](#)
- [Configurar subredes con la CLI](#)

## Requisitos

Cuando actualice las subredes del equilibrador de carga, debe ajustarse a los siguientes requisitos:

- El equilibrador de carga debe tener al menos una subred en todo momento.
- Puede agregar, como máximo, una subred por cada zona de disponibilidad.
- No puede agregar una subred de zona local.

Como hay subredes independientes APIs para añadir y eliminar subredes de un balanceador de cargas, debes tener en cuenta el orden de las operaciones al cambiar las subredes actuales por nuevas subredes para cumplir con estos requisitos. Además, si quiere cambiar todas las subredes del equilibrador de carga, deberá agregar temporalmente una subred de otra zona de disponibilidad. Por ejemplo, si el equilibrador de carga solamente tiene una única zona de disponibilidad y necesita cambiar la subred por otra, deberá agregar primero una subred de otra zona de disponibilidad. A continuación, podrá eliminar la subred de la zona de disponibilidad original (sin que quede menos de una subred), agregar una nueva subred de la zona de disponibilidad original (sin que haya más de una subred por zona de disponibilidad) y, a continuación, eliminar la subred de la segunda zona de disponibilidad (solo si es necesario para realizar el cambio).

## Configurar las subredes con la consola

Utilice el siguiente procedimiento para añadir o eliminar subredes utilizando la consola.

### Para configurar subredes con 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 para abrir su página de detalles.
4. En la pestaña Asignación de redes, seleccione Editar subredes.
5. En la página Editar subredes, en la sección de Asignación de redes, agregue y elimine subredes según sea necesario.
6. Cuando haya finalizado, elija Guardar cambios.

## Configurar subredes con la CLI

Utilice los siguientes ejemplos para añadir o eliminar subredes utilizando la AWS CLI.

Para agregar una subred al equilibrador de carga a través de CLI

Usa el siguiente comando [attach-load-balancer-to-subnets](#) para añadir dos subredes a tu balanceador de carga:

```
aws elb attach-load-balancer-to-subnets --load-balancer-name my-load-balancer --  
subnets subnet-dea770a9 subnet-fb14f6a2
```

En la respuesta, aparecerán todas las subredes del equilibrador de carga. Por ejemplo:

```
{  
  "Subnets": [  
    "subnet-5c11033e",  
    "subnet-dea770a9",  
    "subnet-fb14f6a2"  
  ]  
}
```

Para eliminar una subred mediante el AWS CLI

Usa el siguiente comando [detach-load-balancer-from-subnets](#) para eliminar las subredes especificadas del balanceador de cargas especificado:

```
aws elb detach-load-balancer-from-subnets --load-balancer-name my-Loadbalancer --  
subnets subnet-450f5127
```

En la respuesta, se muestran las subredes restantes del equilibrador de carga. Por ejemplo:

```
{
```

```
"Subnets": [  
    "subnet-15aaab61"  
]  
}
```

## Configurar grupos de seguridad para el equilibrador de carga clásico

Al usar el Consola de administración de AWS para crear un balanceador de cargas, puede elegir un grupo de seguridad existente o crear uno nuevo. Si elige un grupo de seguridad existente, el tráfico debe estar permitido en las dos direcciones en el puerto de oyente y el puerto de comprobación de estado del equilibrador de carga. Si decide crear un grupo de seguridad, la consola agregará automáticamente reglas que permitan todo el tráfico en estos puertos.

[VPC no predeterminada] Si usa AWS CLI la API o crea un balanceador de carga en una VPC no predeterminada, pero no especifica un grupo de seguridad, su balanceador de carga se asocia automáticamente al grupo de seguridad predeterminado de la VPC.

[VPC predeterminada] Si utilizas la API AWS CLI o para crear un balanceador de cargas en tu VPC predeterminada, no podrás elegir un grupo de seguridad existente para tu balanceador de cargas. En su lugar, ELB proporciona un grupo de seguridad con reglas que permiten que todo el tráfico entre en los puertos especificados para el balanceador de cargas. El ELB crea solo uno de estos grupos de seguridad por AWS cuenta, con un nombre con el formato *id* default\_elb\_ (por ejemplo, default\_elb\_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE). Los equilibradores de carga que cree posteriormente en la VPC predeterminada también usarán este grupo de seguridad. No olvide revisar las reglas del grupo de seguridad para asegurarse de que permiten el tráfico en el puerto de oyente y el puerto de comprobación de estado del nuevo equilibrador de carga. Cuando elimine el equilibrador de carga, el grupo de seguridad no se eliminará automáticamente.

Si agrega un oyente a un equilibrador de carga existente, deberá revisar los grupos de seguridad para asegurarse de que el tráfico está permitido en el puerto del nuevo oyente en las dos direcciones.

### Contenido

- [Reglas recomendadas para los grupos de seguridad del equilibrador de carga](#)
- [Asignación de grupos de seguridad a través de la consola](#)
- [Asigne grupos de seguridad mediante el AWS CLI](#)

## Reglas recomendadas para los grupos de seguridad del equilibrador de carga

Los grupos de seguridad de los equilibradores de carga deben permitir que estos se comuniquen con las instancias. Las reglas recomendadas dependen del tipo de equilibrador de carga expuesto a Internet o interno.

### Equilibrador de carga expuesto a Internet

En la tabla siguiente, se muestran las reglas recomendadas entrantes para un equilibrador de carga expuesto a Internet.

origen	Protocolo	Rango de puertos	Comment
0.0.0.0/0	TCP	<i>listener</i>	Permitir todo el tráfico entrante en el puerto del oyente del equilibrador de carga

En la tabla siguiente, se muestran las reglas recomendadas salientes para un equilibrador de carga expuesto a Internet.

Destino	Protocolo	Rango de puertos	Comment
<i>instance security group</i>	TCP	<i>instance listener</i>	Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia
<i>instance security group</i>	TCP	<i>health check</i>	Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado

### Equilibradores de carga internos

En la tabla siguiente, se muestran las reglas recomendadas entrante para un equilibrador de carga interno.

origen	Protocolo	Rango de puertos	Comment
<b>VPC CIDR</b>	TCP	<i>Listener</i>	Permitir el tráfico entrante del CIDR de VPC en el puerto del oyente del equilibrador de carga

En la tabla siguiente, se muestran las reglas recomendadas saliente para un equilibrador de carga interno.

Destino	Protocolo	Rango de puertos	Comment
<i>instance security group</i>	TCP	<i>instance listener</i>	Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia
<i>instance security group</i>	TCP	<i>health check</i>	Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado

## Asignación de grupos de seguridad a través de la consola

Utilice el siguiente procedimiento para cambiar los grupos de seguridad asociados al equilibrador de carga.

Para actualizar un grupo de seguridad asignado al 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 Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Seguridad, seleccione Editar.
5. En la página Editar grupos de seguridad, en Grupos de seguridad, agregue o elimine grupos de seguridad según sea necesario.

Puede agregar hasta cinco grupos de seguridad.

6. Cuando haya finalizado, elija Guardar cambios.

## Asigne grupos de seguridad mediante el AWS CLI

Use el siguiente comando [apply-security-groups-to-load-balancer](#) para asociar un grupo de seguridad a un balanceador de cargas. Los grupos de seguridad especificados sobrescribe los grupos de seguridad asociados anteriormente.

```
aws elb apply-security-groups-to-load-balancer --load-balancer-name my-loadbalancer --  
security-groups sg-53fae93f
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "SecurityGroups": [  
    "sg-53fae93f"  
  ]  
}
```

## Configura la red ACLs para tu Classic Load Balancer

La lista de control de acceso (ACL) de red predeterminada de una VPC permite todo el tráfico de entrada y salida. Si creas una red personalizada ACLs, debes agregar reglas que permitan que el balanceador de carga y las instancias se comuniquen.

Las reglas recomendadas para la subred del equilibrador de carga dependerán del tipo de equilibrador de carga expuesto a Internet o interno.

### Equilibrador de carga expuesto a Internet

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

origen	Protocolo	Rango de puertos	Comment
0.0.0.0/0	TCP	<i>listener</i>	Permitir todo el tráfico entrante en el puerto del oyente del equilibrador de carga

origen	Protocolo	Rango de puertos	Comment
<b>VPC CIDR</b>	TCP	1024-65535	Permitir el tráfico entrante en el CIDR de la VPC a través de los puertos efímeros

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

Destino	Protocolo	Rango de puertos	Comment
<b>VPC CIDR</b>	TCP	<i>instance listener</i>	Permite todo el tráfico de salida en el puerto de oyente de la instancia
<b>VPC CIDR</b>	TCP	<i>health check</i>	Permite todo el tráfico de salida en el puerto de comprobación de estado
0.0.0.0/0	TCP	1024-65535	Permite todo el tráfico de salida en los puertos efímeros

## Equilibrador de carga interno

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

origen	Protocolo	Rango de puertos	Comment
<b>VPC CIDR</b>	TCP	<i>Listener</i>	Permitir el tráfico entrante del CIDR de VPC en el puerto del oyente del equilibrador de carga
<b>VPC CIDR</b>	TCP	1024-65535	Permitir el tráfico entrante en el CIDR de la VPC a través de los puertos efímeros

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

Destino	Protocolo	Rango de puertos	Comment
<i>VPC CIDR</i>	TCP	<i>instance listener</i>	Permite el tráfico de salida dirigido al CIDR de la VPC en el puerto de oyente de la instancia
<i>VPC CIDR</i>	TCP	<i>health check</i>	Permite el tráfico de salida en el CIDR de la VPC del puerto de comprobación de estado
<i>VPC CIDR</i>	TCP	1024-65535	Permitir el tráfico de salida en el CIDR de la VPC a través de los puertos efímeros

## Configuración de un nombre de dominio personalizado para el equilibrador de carga clásico

Cada equilibrador de carga clásico recibe un nombre predeterminado del sistema de nombres de dominio (DNS). Este nombre DNS incluye el nombre de la AWS región en la que se creó el balanceador de cargas. Por ejemplo, si crea un equilibrador de carga denominado `my-loadbalancer` en la región Oeste de EE. UU. (Oregón), el equilibrador de carga recibe un nombre de DNS del tipo `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com`. Para obtener acceso al sitio web en las instancias, debe pegar este nombre de DNS en el campo de direcciones de un navegador web. Sin embargo, este nombre de DNS no les resulta fácil de recordar y utilizar a sus clientes.

Si prefiere utilizar un nombre de DNS descriptivo para el equilibrador de carga (por ejemplo, `www.example.com`) en lugar del nombre de DNS predeterminado, puede crear un nombre de dominio personalizado y asociárselo al nombre de DNS del equilibrador de carga. Cuando un cliente realiza una solicitud utilizando este nombre de dominio personalizado, el servidor DNS lo resuelve para hallar el nombre de DNS del equilibrador de carga.

### Contenido

- [Asociación del nombre de dominio personalizado al nombre del equilibrador de carga](#)

- [Uso de la conmutación por error de DNS de Route 53 para el equilibrador de carga](#)
- [Desasociación del nombre de dominio personalizado del equilibrador de carga](#)

## Asociación del nombre de dominio personalizado al nombre del equilibrador de carga

En primer lugar, si aún no lo ha hecho, registre su nombre de dominio. La Internet Corporation for Assigned Names and Numbers (ICANN, Corporación de Internet para la Asignación de Nombres y Números) administra los nombres de dominios de Internet. Los nombres de dominios se registran mediante un registrador de nombres de dominio, una organización acreditada por la ICANN que administra el registro de los nombres de dominios. En el sitio web de su registrador, se detallarán las instrucciones y la información sobre los precios del registro del nombre de dominio. Para obtener más información, consulte los siguientes recursos:

- Para registrar el nombre de un dominio mediante Amazon Route 53, consulte [Registro de nombres de dominio mediante Route 53](#) en la Guía para desarrolladores de Amazon Route 53.
- Para obtener una lista de registradores acreditados, consulte [Lista de registradores acreditados](#).

A continuación, utilice su servicio DNS (por ejemplo, su registrador de dominio) para crear un registro CNAME y dirigir las consultas al equilibrador de carga. Para obtener más información, consulte la documentación de su servicio de DNS.

También puede usar Route 53 como su servicio DNS. Deberá crear una zona alojada, que contiene información sobre cómo enrutar en Internet el tráfico para el dominio, así como un conjunto de registros de recursos de alias, que dirige las consultas al equilibrador de carga. Route 53 no aplica cargos por las consultas de DNS de los conjuntos de registros de alias y los puede utilizar para dirigir las consultas de DNS al equilibrador de carga para el vértice de zona del dominio (por ejemplo, example.com). A fin de obtener información sobre cómo transferir los servicios DNS para los dominios existentes a Route 53, consulte [Configuración de Route 53 como un servicio DNS](#) en la Guía para desarrolladores de Amazon Route 53.

Por último, cree una zona alojada y un conjunto de registros de alias para el dominio desde Route 53. Para obtener más información, consulte [Enrutamiento del tráfico a un equilibrador de carga](#) en la Guía para desarrolladores de Amazon Route 53.

## 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 las EC2 instancias registradas del balanceador de carga para determinar si están disponibles. Si no hay EC2 instancias en buen estado registradas en el balanceador de carga, o si el balanceador de carga en sí está en mal estado, Route 53 dirige el tráfico a otro recurso disponible, como un balanceador 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.

### Uso de Evaluate Target Health

- Cuando Evaluate Target Health se establece en Yes en un registro de alias para un equilibrador de carga clásico, Route 53 evalúa el estado del recurso especificado por el valor de alias `target`. Para un equilibrador de carga clásico, Route 53 utiliza las comprobaciones de estado de la instancia asociadas al equilibrador de carga.
- Cuando al menos una de las instancias registradas en un equilibrador de carga clásico está en buen estado, Route 53 marca el estado del registro de alias como en buen estado. A continuación, Route 53 devuelve los registros de acuerdo con su política de enrutamiento. Si se utiliza la política de enrutamiento de conmutación por error, Route 53 devuelve el registro principal.
- Cuando todas las instancias registradas para un equilibrador de carga clásico están en mal estado, Route 53 marca el registro de alias como en mal estado. A continuación, Route 53 devuelve los registros de acuerdo con su política de enrutamiento. Si se utiliza la política de enrutamiento de conmutación por error, Route 53 devuelve el registro secundario.

Para obtener más información, consulte [Configuración de la conmutación por error a nivel de DNS](#) en la Guía para desarrolladores de Amazon Route 53.

## Desasociación del nombre de dominio personalizado del equilibrador de carga

Puede desasociar el nombre de dominio personalizado de una instancia del equilibrador de carga. Para ello, lo primero que debe hacer es eliminar los conjuntos de registro de recursos de la zona alojada y, a continuación, eliminar la zona alojada. Para obtener más información, consulte [Edición de registros](#) y [Eliminación de una zona alojada pública](#) en la Guía para desarrolladores de Amazon Route 53.

# Oyentes para el equilibrador de carga clásico

Antes de empezar a usar ELB, debe configurar uno o más oyentes para su Classic Load Balancer. Un oyente es un proceso que verifica solicitudes de conexión. Se configura con un protocolo y un puerto para las conexiones frontend (del cliente al equilibrador de carga) y un protocolo y un puerto para las conexiones backend (del equilibrador de carga a la instancia de backend).

ELB admite los siguientes protocolos:

- HTTP
- HTTPS (HTTP seguro)
- TCP
- SSL (TCP seguro)

El protocolo HTTPS utiliza el protocolo SSL para establecer conexiones seguras a través de la capa HTTP. También puede utilizar el protocolo SSL para establecer conexiones seguras a través de la capa TCP.

Si la conexión frontend utiliza TCP o SSL, las conexiones backend pueden utilizar TCP o SSL. Si la conexión frontend utiliza HTTP o HTTPS, las conexiones backend pueden utilizar HTTP o HTTPS.

Las instancias backend pueden escuchar los puertos 1-65535.

Los equilibradores de carga pueden oyente en los siguientes puertos: 1-65535

## Contenido

- [Protocolos](#)
- [Oyentes HTTPS/SSL](#)
- [Configuraciones de oyentes para los equilibradores de carga clásicos](#)
- [Encabezados HTTP y equilibradores de carga clásicos](#)

## Protocolos

La comunicación para una aplicación web típica atraviesa capas de hardware y software. Cada capa ofrece una función de comunicación específica. El control de la función de comunicación se transfiere

de una capa a la siguiente, de forma secuencial. El modelo de interconexión de sistemas abiertos (OSI) define un marco para implementar un formato de comunicación estándar en estas capas, que se denomina protocolo. Para obtener más información, consulte [OSI model](#) en Wikipedia.

Cuando se utiliza el ELB, se necesitan conocimientos básicos de la capa 4 y la capa 7. La capa 4 es la capa de transporte que describe la conexión del protocolo de control de transmisión (TCP) entre el cliente y la instancia backend a través del equilibrador de carga. La capa 4 es el nivel más bajo que el equilibrador de carga puede configurar. La capa 7 es la capa de aplicaciones que describe el uso de las conexiones del protocolo de transferencia de hipertexto (HTTP) y HTTP seguro (HTTPS) desde los clientes al equilibrador de carga y desde este hasta la instancia backend.

El protocolo de capa de conexión segura (SSL) se utiliza principalmente para cifrar datos confidenciales que se transmiten a través de redes que no son seguras, como Internet. El protocolo SSL establece una conexión segura entre un cliente y el servidor backend. Además, se asegura de que todos los datos transferidos entre el cliente y el servidor sean privados e íntegros.

## Protocolo TCP/SSL

Cuando se utiliza TCP (capa 4) para las conexiones frontend y backend, el equilibrador de carga reenvía las solicitudes a las instancias backend sin modificar los encabezados. Una vez que el equilibrador de carga recibe la solicitud, intenta abrir una conexión TCP con la instancia backend en el puerto especificado en la configuración del oyente.

Dado que los equilibradores de carga interceptan el tráfico entre los clientes y las instancias backend, los registros de acceso desde la instancia backend contienen la dirección IP del equilibrador de carga, y no la del cliente de origen. Puede habilitar Proxy Protocol, lo que agrega un encabezado con la información de conexión del cliente, como la dirección IP de origen, la dirección IP de destino y los números de puerto. El encabezado se enviará a la instancia backend como parte de la solicitud. Puede analizar la primera línea de la solicitud para recuperar la información de conexión. Para obtener más información, consulte [Configuración del protocolo de proxy del Equilibrador de carga clásico](#).

Cuando se utiliza esta configuración, no se reciben cookies de sesiones persistentes ni encabezados X-Forwarded.

## Protocolo HTTP/HTTPS

Cuando se utiliza HTTP (capa 7) para las conexiones frontend y backend, el equilibrador de carga analiza los encabezados de la solicitud antes de enviar la solicitud a las instancias backend.

Por cada instancia registrada y en buen estado detrás de un HTTP/HTTPS balanceador de cargas, ELB abre y mantiene una o más conexiones TCP. Estas conexiones garantizan que siempre haya una conexión establecida y preparada para recibir solicitudes HTTP/HTTPS.

Las solicitudes y respuestas HTTP utilizan campos de encabezado para enviar información sobre los mensajes HTTP. El ELB admite encabezados. `X-Forwarded-For` 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 encabezado de solicitud `X-Forwarded-For`. Para obtener más información, consulte [X-Forwarded-For](#).

Cuando se utiliza HTTP/HTTPS, se pueden habilitar las sesiones persistentes en el equilibrador de carga. Una sesión persistente vincula una sesión del usuario a una instancia backend concreta. Con ello se garantiza que todas las solicitudes procedentes de ese usuario durante la sesión se envíen a la misma instancia backend. Para obtener más información, consulte [Configuración de sesiones persistentes para el Equilibrador de carga clásico](#).

El equilibrador de carga no admite todas las extensiones HTTP. Puede ser necesario utilizar un oyente TCP si el equilibrador de carga no consigue terminar la solicitud a causa de métodos, códigos de respuesta u otras implementaciones de HTTP 1.0/1.1 no estándar inesperados.

## Oyentes HTTPS/SSL

Puede crear un equilibrador de carga con las siguientes características de seguridad.

### Certificados de servidor SSL

Si utiliza HTTPS o SSL para las conexiones frontend, debe implementar un certificado X.509 (certificado de servidor SSL) en el equilibrador de carga. El equilibrador de carga descifra las solicitudes de los clientes antes de enviarlas a las instancias backend (esto se denomina terminación SSL). Para obtener más información, consulte [Certificados SSL/TLS para equilibradores de carga clásicos](#).

Si no desea que el equilibrador de carga controle la terminación SSL (lo que se denomina descarga de SSL), puede utilizar TCP para las conexiones frontend y backend e implementar certificados en las instancias registradas que controlan solicitudes.

## Negociación SSL

ELB proporciona configuraciones de negociación de SSL predefinidas que se utilizan para la negociación de SSL cuando se establece una conexión entre un cliente y el balanceador de cargas. Las configuraciones de la negociación SSL proporcionan compatibilidad con una amplia variedad de clientes y utilizan algoritmos criptográficos de alta seguridad denominados cifrados. Sin embargo, algunos casos de uso podrían requerir que se cifren todos los datos de la red y admitir solo algunos cifrados. Algunos estándares de conformidad y seguridad (como PCI, SOX, etc.) podrían requerir un conjunto específico de protocolos y cifrados de los clientes para garantizar que se cumplan los estándares de seguridad. En estos casos, puede crear una configuración de negociación SSL personalizada que se ajuste a sus requisitos específicos. Los cifrados y protocolos deben surtir efecto en un plazo de 30 segundos. Para obtener más información, consulte [Configuraciones de negociación SSL para el equilibrador de carga clásico](#).

## Autenticación del servidor backend

Si utiliza HTTPS o SSL para las conexiones backend, puede habilitar la autenticación de las instancias registradas. A continuación, puede utilizar el proceso de autenticación para asegurarse de que las instancias acepten únicamente la comunicación cifrada y de que cada instancia registrada tenga la clave pública correcta.

Para obtener más información, consulte [Configure Back-end Server Authentication](#).

## Configuraciones de oyentes para los equilibradores de carga clásicos

En la siguiente tabla se describen las posibles configuraciones de los oyentes HTTP y HTTPS para un Equilibrador de carga clásico.

Caso de uso	Protocolo frontend	Opciones frontend	Protocolo backend	Opciones backend	Notas
Equilibrador de carga HTTP básico	HTTP	N/D	HTTP	N/D	<ul style="list-style-type: none"><li>Admite los <a href="#">encabezados X-Forwarded</a>.</li></ul>

Caso de uso	Protocolo frontend	Opciones frontend	Protocolo backend	Opciones backend	Notas
Proteja un sitio web o una aplicación con ELB para evitar el descifrado SSL	HTTPS	<a href="#">Negociación SSL</a>	HTTP	N/D	<ul style="list-style-type: none"> <li>Admite los <a href="#">encabezados X-Forwarded</a>.</li> <li>Requiere implementar un <a href="#">certificado SSL</a> en el equilibrador de carga</li> </ul>
Proteja el sitio web o la aplicación mediante cifrado end-to-end	HTTPS	<a href="#">Negociación SSL</a>	HTTPS	Autenticación backend	<ul style="list-style-type: none"> <li>Admite los <a href="#">encabezados X-Forwarded</a>.</li> <li>Requiere implementar <a href="#">certificados SSL</a> en el equilibrador de carga y en las instancias registradas</li> </ul>

En la siguiente tabla se describen las posibles configuraciones de los oyentes TCP y SSL para un Equilibrador de carga clásico.

Caso de uso	Protocolo frontend	Opciones frontend	Protocolo backend	Opciones backend	Notas
Equilibrador de carga TCP básico	TCP	N/D	TCP	N/D	<ul style="list-style-type: none"> <li>Admite el <a href="#">encabezado Proxy Protocol</a></li> </ul>
Proteja el sitio web o la aplicación mediante ELB para evitar el descifrado SSL	SSL	<a href="#">Negociación SSL</a>	TCP	N/D	<ul style="list-style-type: none"> <li>Requiere implementar un <a href="#">certificado SSL</a> en el equilibrador de carga</li> <li>Admite el <a href="#">encabezado Proxy Protocol</a></li> </ul>
Proteja el sitio web o la aplicación mediante el cifrado con ELB end-to-end	SSL	<a href="#">Negociación SSL</a>	SSL	Autenticación backend	<ul style="list-style-type: none"> <li>Requiere implementar <a href="#">certificados SSL</a> en el equilibrador de carga y en las instancias registradas</li> <li>No inserte encabezados SNI en las conexiones</li> </ul>

Caso de uso	Protocolo frontend	Opciones frontend	Protocolo backend	Opciones backend	Notas
					<ul style="list-style-type: none"> <li>• Soporta SSL</li> <li>• Soporta backend</li> <li>• No admite el encabezado Proxy Protocol</li> </ul>

## Encabezados HTTP y equilibradores de carga clásicos

Las solicitudes y respuestas HTTP utilizan campos de encabezado para enviar información sobre los mensajes HTTP. 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 (y que se agregan automáticamente) que se suelen utilizar en las aplicaciones. Algunos de los encabezados HTTP no estándar tienen un prefijo X-Forwarded. Los equilibradores de carga clásicos 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.

### Requisitos previos

- Confirme que la configuración del oyente admite los encabezados X-Forwarded. Para obtener más información, consulte [Configuraciones de oyentes para los equilibradores de carga clásicos](#).
- Configure el servidor web de forma que registre las direcciones IP del cliente.

### Encabezados X-Forwarded

- [X-Forwarded-For](#)
- [X-Forwarded-Proto](#)
- [X-Forwarded-Port](#)

## X-Forwarded-For

El encabezado de solicitud `X-Forwarded-For` se agrega automáticamente y 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 encabezado de solicitud `X-Forwarded-For`. ELB almacena la dirección IP del cliente en el encabezado de la `X-Forwarded-For` solicitud y pasa el encabezado a su servidor. Si el encabezado de solicitud `X-Forwarded-For` no se incluye en la solicitud, 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. La dirección más a la izquierda es la IP del cliente en la que se realizó la solicitud por primera vez. Le sigue cualquier identificador de proxy posterior, en cadena.

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`

El siguiente es 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`

## 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`. ELB almacena el protocolo utilizado entre el

cliente y el balanceador de carga en el encabezado de la X-Forwarded-Proto solicitud y 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.

# Oyentes HTTPS para el equilibrador de carga clásico

Puedes crear un balanceador de cargas que utilice el SSL/TLS protocolo para las conexiones cifradas (también conocido como descarga SSL). Esta función permite cifrar el tráfico entre tu balanceador de cargas y los clientes que inician las sesiones HTTPS, así como para las conexiones entre tu balanceador de cargas y tus instancias. EC2

ELB utiliza configuraciones de negociación de Secure Sockets Layer (SSL), conocidas como políticas de seguridad, para negociar las conexiones entre los clientes y el balanceador de cargas. Cuando las usa HTTPS/SSL para sus conexiones front-end, puede usar una política de seguridad predefinida o una política de seguridad personalizada. Para ello, debe implementar un certificado SSL en el equilibrador de carga. El equilibrador de carga usará este certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de enviárselas a las instancias. El equilibrador de carga utiliza un conjunto de cifrado estático para las conexiones backend. Si lo desea, también puede habilitar la autenticación de las instancias.

Los equilibradores de carga clásicos no admiten la indicación de nombre de servidor (SNI). En su lugar, puede utilizar una de las siguientes alternativas:

- Implemente un certificado en el balanceador de cargas y añada un nombre alternativo del sujeto (SAN) para cada sitio web adicional. SANs le permiten proteger varios nombres de host mediante un único certificado. Consulte con su proveedor de certificados para obtener más información sobre el número de certificados SANs que admiten por certificado y sobre cómo añadirlos y eliminarlos SANs.
- Utilice oyentes TCP en el puerto 443 de las conexiones frontend y backend. El balanceador de cargas tramita la solicitud tal cual, para que puedas gestionar la terminación de HTTPS en la EC2 instancia.

Los equilibradores de carga clásicos no admiten la autenticación TLS mutua (MTLs). Para la compatibilidad con mTLS, cree un oyente TCP. El balanceador de cargas tramita la solicitud tal cual, para que puedas implementar mTLS en la instancia. EC2

## Contenido

- [Certificados SSL/TLS para equilibradores de carga clásicos](#)
- [Configuraciones de negociación SSL para el equilibrador de carga clásico](#)
- [Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos](#)

- [Creación de un equilibrador de carga clásico con un oyente HTTPS](#)
- [Configuración de un oyente HTTPS para el equilibrador de carga clásico](#)
- [Reemplazo del certificado SSL del equilibrador de carga clásico](#)
- [Actualización de la configuración de la negociación SSL del equilibrador de carga clásico](#)

## Certificados SSL/TLS para equilibradores de carga clásicos

Si utiliza HTTPS (SSL o TLS) con el oyente frontend, debe implementar un certificado SSL/TLS en el equilibrador de carga. El equilibrador de carga usará el certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de enviarlas a las instancias.

Los protocolos TLS y SSL utilizan un certificado X.509 (certificado de servidor SSL/TLS) para autenticar la aplicación cliente y la aplicación backend. Un certificado X.509 es un formulario de identificación digital emitido por una entidad de certificación (CA) y contiene información de identificación, un periodo de validez, una clave pública, un número de serie y la firma digital del emisor.

Puede crear un certificado mediante AWS Certificate Manager o una herramienta que admita los protocolos SSL y TLS, como OpenSSL. Podrá especificar este certificado cuando cree o actualice un oyente HTTPS para el equilibrador de carga. Al crear un certificado para utilizarlo con el equilibrador de carga, debe especificar un nombre de dominio.

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. Si no coinciden, no se cifrará el tráfico, ya que no se puede verificar la conexión TLS.

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 comodín aparecerá en el campo Sujeto y en la extensión Nombre alternativo del sujeto del certificado. Para obtener más información sobre certificados públicos, consulte [Solicitud de un certificado público](#) en la Guía del usuario de AWS Certificate Manager .

## Cree o importe un certificado mediante SSL/TLS AWS Certificate Manager

Te recomendamos que utilices AWS Certificate Manager (ACM) para crear o importar certificados para tu balanceador de cargas. ACM se integra con ELB para que puedas implementar el certificado en tu balanceador de cargas. Para poder implementar un certificado en el equilibrador de carga, el certificado debe estar en la misma región que el equilibrador de carga. Para obtener más información, consulte [Solicitud de un certificado público](#) o [Importación de certificados](#) en la Guía del usuario de AWS Certificate Manager .

Para permitir que un usuario pueda implementar el certificado en el equilibrador de carga a través de la Consola de administración de AWS, debe permitir el acceso a la acción de la API `ListCertificates` de ACM. Para obtener más información, consulte [Listado de certificados](#) en la Guía del usuario de AWS Certificate Manager .

### Important

No puede instalar certificados con claves RSA de 4096 bits ni claves EC en el equilibrador de carga a través de la integración con ACM. Debe cargar certificados con claves RSA de 4096 bits o claves EC en IAM para utilizarlos con el equilibrador de carga.

## Importe un certificado mediante IAM SSL/TLS

Si no utiliza ACM, puede utilizar SSL/TLS herramientas, como OpenSSL, para crear una solicitud de firma de certificado (CSR), conseguir que una CA firme la CSR para generar un certificado y cargar el certificado en IAM. Para obtener más información, consulte [Working with Server Certificates](#) (Trabajar con certificados de servidores) en la Guía para el usuario de IAM.

## Configuraciones de negociación SSL para el equilibrador de carga clásico

El ELB 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 balanceador de cargas. Una política de seguridad es una combinación de protocolos SSL, cifrados SSL y la opción de preferencia del orden del servidor. Para obtener más información acerca de cómo configurar una conexión SSL para el equilibrador de carga, consulte [Oyentes para el equilibrador de carga clásico](#).

### Contenido

- [Políticas de seguridad](#)
- [Protocolos SSL](#)
- [Preferencia del orden del servidor](#)
- [Cifrados SSL](#)
- [Conjunto de cifrado para conexiones backend](#)

## Políticas de seguridad

Una política de seguridad determina qué cifrados y protocolos se admiten durante las negociaciones SSL entre un cliente y un equilibrador de carga. Puede configurar los equilibradores de carga clásicos para que utilicen políticas de seguridad predefinidas o personalizadas.

Tenga en cuenta que un certificado proporcionado por AWS Certificate Manager (ACM) contiene una clave pública RSA. Por lo tanto, si utiliza un certificado proporcionado por ACM, debe incluir en la política de seguridad un cifrado que utilice RSA; de lo contrario, la conexión TLS fallará.

### Políticas de seguridad predefinidas

Los nombres de la versión más reciente de las políticas de seguridad predefinidas contienen información sobre el año y el mes de lanzamiento. Por ejemplo, la política de seguridad predefinida que se utiliza de forma predeterminada es `ELBSecurityPolicy-2016-08`. Siempre que se publica una nueva política de seguridad predefinida, se puede actualizar la configuración para utilizarla.

Para obtener información sobre los protocolos y cifrados habilitados para las políticas de seguridad predefinidas, consulte [Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos](#).

### Políticas de seguridad personalizadas

Puede crear una configuración de negociación personalizada con los cifrados y protocolos que necesite. Por ejemplo, es posible que algunos estándares de conformidad y seguridad (como PCI y SOC) necesiten un conjunto específico de protocolos y cifrados que garanticen que se cumplen los estándares de seguridad. En estos casos, puede crear una política de seguridad personalizada que se ajuste a estos estándares.

Para obtener información sobre la creación de una política de seguridad personalizada, consulte [Actualización de la configuración de la negociación SSL del equilibrador de carga clásico](#).

## Protocolos SSL

El protocolo SSL 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.

Capa de conexión segura (SSL) y Transport Layer Security (TLS) son protocolos criptográficos que se usan para cifrar los datos confidenciales a través de redes que no son seguras, como Internet.

El protocolo TLS es una versión más reciente del protocolo SSL. En la documentación del ELB, nos referimos a los protocolos SSL y TLS como protocolo SSL.

### Protocolo recomendado

Recomendamos el TLS 1.2, que se utiliza en la ELBSecurity política de seguridad predefinida TLS-1-2-2017-01. También puede usar TLS 1.2 en sus políticas de seguridad personalizadas. La política de seguridad predeterminada es compatible con TLS 1.2 y versiones anteriores de TLS, por lo que es menos segura que la política TLS-1-2-2017-01. ELBSecurity

### Protocolo obsoleto

Si anteriormente habilitó el protocolo SSL 2.0 en una política personalizada, le recomendamos que actualice la política de seguridad a una de las políticas de seguridad predefinidas que se usan de forma predeterminada.

## Preferencia del orden del servidor

ELB admite la opción de preferencia de orden de servidor para negociar las conexiones entre un cliente y un balanceador de cargas. Durante el proceso de negociación de conexiones SSL, 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 cifrado que se va a seleccionar para la conexión SSL será el primero de la lista del cliente que coincida con uno de los cifrados del equilibrador de carga. Si el equilibrador de carga está configurado para admitir la preferencia del orden del servidor, seleccionará el primer cifrado de su lista que se encuentre también en la lista del cliente. De este modo, el equilibrador de carga determina el cifrado que se utiliza con la conexión SSL. Si no se admite la preferencia del orden del servidor, el orden de cifrados presentado por el cliente se utiliza para negociar las conexiones entre el cliente y el equilibrador de carga.

## Cifrados SSL

Un cifrado SSL es un algoritmo de cifrado que usa claves de cifrado para crear un mensaje codificado. Los protocolos SSL usan diversos cifrados SSL para cifrar los datos a través de Internet.

Tenga en cuenta que un certificado proporcionado por AWS Certificate Manager (ACM) contiene una clave pública RSA. Por lo tanto, si utiliza un certificado proporcionado por ACM, debe incluir en la política de seguridad un cifrado que utilice RSA; de lo contrario, la conexión TLS fallará.

El ELB admite los siguientes cifrados para su uso con los balanceadores de carga clásicos. Las políticas SSL predefinidas utilizan un subconjunto de estos cifrados. Todos estos cifrados están disponibles para utilizarse en las políticas personalizadas. Le recomendamos que utilice solo los cifrados incluidos en la política de seguridad predeterminada (están marcados con un asterisco). Muchos de los demás cifrados no son seguros y, si los utiliza, deberá hacerlo bajo su propia responsabilidad.

## Cifrados

- ECDHE-ECDSA- -GCM- \* AES128 SHA256
- ECDHE-RSA- AES128 -GCM- \* SHA256
- ECDHE-ECDSA- AES128 - \* SHA256
- ECDHE-RSA- AES128 - \* SHA256
- ECDHE-ECDSA AES128 - -SHA \*
- ECDHE-RSA- AES128 -SHA \*
- DHE-RSA- AES128 -SHA
- ECDHE-ECDSA- -GCM- \* AES256 SHA384
- ECDHE-RSA- AES256 -GCM- \* SHA384
- ECDHE-ECDSA- AES256 - \* SHA384
- ECDHE-RSA- AES256 - \* SHA384
- ECDHE-RSA AES256 - -SHA \*
- ECDHE-ECDSA- AES256 -SHA \*
- AES128-GCM- \* SHA256
- AES128-SHA256 \*
- AES128-SHA \*
- AES256-GCM- \* SHA384
- AES256-SHA256 \*
- AES256-SHA \*

- DHE-DSS- -SHA AES128
- CAMELLIA128-SHA
- EDH-RSA-DES- -SHA CBC3
- DES- CBC3 -SHA
- ECDHE-RSA- -SHA RC4
- RC4-SHA
- ECDHE-ECDSA- -SHA RC4
- DHE-DSS- -GCM- AES256 SHA384
- DHE-RSA- AES256 -GCM- SHA384
- DHE-RSA- AES256 - SHA256
- DHE-DSS- AES256 - SHA256
- DHE-RSA- -SHA AES256
- DHE-DSS- AES256 -SHA
- DHE-RSA- CAMELLIA256 -SHA
- DHE-DSS- CAMELLIA256 -SHA
- CAMELLIA256-SHA
- EDH-DSS-DE-SHA CBC3
- DHE-DSS- AES128 -GCM- SHA256
- DHE-RSA- AES128 -GCM- SHA256
- DHE-RSA- AES128 - SHA256
- DHE-DSS- AES128 - SHA256
- DHE-RSA- -SHA CAMELLIA128
- DHE-DSS- CAMELLIA128 -SHA
- ADH- -GCM- AES128 SHA256
- ADH- -SHA AES128
- ADH- - AES128 SHA256
- ADH- AES256 -GCM- SHA384
- ADH- -SHA AES256
- ADH- - AES256 SHA256

- ADH- CAMELLIA128 -SHA
- ADH- -SHA CAMELLIA256
- ADH-DES- -SHA CBC3
- ADH-DES-CBC-SHA
- ADH- - RC4 MD5
- ADH-SEED-SHA
- DES-CBC-SHA
- DHE-DSS-SEED-SHA
- DHE-RSA-SEED-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- IDEA-CBC-SHA
- RC4-MD5
- SEED-SHA
- DES- CBC3 - MD5
- DES-CBC- MD5
- RC2-CBC- MD5
- PSK- -CBC-SHA AES256
- PSK-3DES-EDE-CBC-SHA
- KRB5CBC3-DES- -SHA
- KRB5-DES- - CBC3 MD5
- PSK- -CBC-SHA AES128
- PSK- RC4 -SHA
- KRB5- -SHA RC4
- KRB5-RC4-MD5
- KRB5-DES-CBC-SHA
- KRB5-DES-CBC- MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA

- EXP-ADH-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP- -CBC- RC2 MD5
- EXP- - -CBC-SHA KRB5 RC2
- EXP KRB5 - -DE-CBC-SHA
- EXP- - -CBC- KRB5 RC2 MD5
- EXP- -DES-CBC- KRB5 MD5
- RC4EXP-ADH- - MD5
- EXP- - RC4 MD5
- EXP- - -SHA KRB5 RC4
- EXP- - - KRB5 RC4 MD5

\* Estos son los cifrados incluidos en la política de seguridad predeterminada, ELBSecurity Policy-2016-08.

## Conjunto de cifrado para conexiones backend

Los equilibradores de carga utilizan un conjunto de cifrado estático con las conexiones backend. Si su Equilibrador de carga clásico y las instancias registradas no pueden negociar una conexión, incluya uno de los siguientes cifrados.

- AES256-GCM- SHA384
- AES256-SHA256
- AES256-SHA
- CAMELLIA256-SHA
- AES128-GCM- SHA256
- AES128-SHA256
- AES128-SHA
- CAMELLIA128-SHA
- RC4-SHA
- DES- -SHA CBC3

- DES-CBC-SHA
- DHE-DSS- -GCM- AES256 SHA384
- DHE-RSA- AES256 -GCM- SHA384
- DHE-RSA- AES256 - SHA256
- DHE-DSS- AES256 - SHA256
- DHE-RSA- -SHA AES256
- DHE-DSS- AES256 -SHA
- DHE-RSA- CAMELLIA256 -SHA
- DHE-DSS- CAMELLIA256 -SHA
- DHE-DSS- -GCM- AES128 SHA256
- DHE-RSA- AES128 -GCM- SHA256
- DHE-RSA- AES128 - SHA256
- DHE-DSS- AES128 - SHA256
- DHE-RSA- -SHA AES128
- DHE-DSS- AES128 -SHA
- DHE-RSA- CAMELLIA128 -SHA
- DHE-DSS- CAMELLIA128 -SHA
- CBC3EDH-RSA-DES-SHA
- CBC3EDH-DSS-DE-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA

## Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos

Puede elegir una de las políticas de seguridad predefinidas para los oyentes HTTPS/SSL. Puede utilizar una de las políticas `ELBSecurityPolicy-TLS` para ajustarse a los estándares de seguridad y conformidad que requieren que se deshabiliten algunas versiones del protocolo TLS. Como opción, puede crear una política de seguridad personalizada. Para obtener más información, consulte [Actualización de la configuración de negociación SSL](#).

Los cifrados basados en RSA y DSA son específicos del algoritmo de firma que se utiliza para crear un certificado SSL. Asegúrese de crear un certificado SSL utilizando un algoritmo de firma basado en los cifrados que estén habilitados para su política de seguridad.

Si selecciona una política que tenga habilitada la preferencia del orden del servidor, el equilibrador de carga utilizará los cifrados en el orden en el que se especifiquen aquí para negociar las conexiones entre el cliente y el equilibrador de carga. De lo contrario, el equilibrador de carga utilizará los cifrados en el orden en el que los presenta el cliente.

En las siguientes secciones se describen las políticas de seguridad predefinidas más recientes de los equilibradores de carga clásicos, junto con los protocolos y cifrados SSL habilitados. También puede describir las políticas predefinidas mediante el [describe-load-balancer-policies](#) comando.

 Tip

Esta información solo se aplica a los equilibradores de carga clásicos. Para obtener información que se aplique a los otros equilibradores de carga, consulte [Políticas de seguridad para el equilibrador de carga de aplicación](#) y [Políticas de seguridad para el equilibrador de carga de red](#).

## Contenido

- [Protocolos por política](#)
- [Cifrados por política](#)
- [Políticas por cifrado](#)

## Protocolos por política

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

Políticas de seguridad	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolítica-TLS-1-2-2017-01	Sí	No	No
ELBSecurityPolítica-TLS-1-1-2017-01	Sí	Sí	No

Políticas de seguridad	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolítica-2016-08	Sí	Sí	Sí
ELBSecurityPolítica-2015-05	Sí	Sí	Sí
ELBSecurityPolítica-2015-03	Sí	Sí	Sí
ELBSecurityPolítica-2015-02	Sí	Sí	Sí

## Cifrados por política

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

Política de seguridad	Cifrados
ELBSecurityPolítica-TLS-1-2-2017-01	<ul style="list-style-type: none"> <li>• ECDHE-ECDSA- -GCM- AES128 SHA256</li> <li>• ECDHE-RSA- AES128 -GCM- SHA256</li> <li>• ECDHE-ECDSA- AES128 - SHA256</li> <li>• ECDHE-RSA- - AES128 SHA256</li> <li>• ECDHE-ECDSA- -GCM AES256 - SHA384</li> <li>• ECDHE-RSA- AES256 -GCM- SHA384</li> <li>• ECDHE-ECDSA- AES256 - SHA384</li> <li>• ECDHE-RSA- - AES256 SHA384</li> <li>• AES128-GCM- SHA256</li> <li>• AES128-SHA256</li> <li>• AES256-GCM- SHA384</li> <li>• AES256-SHA256</li> </ul>
ELBSecurityPolítica-TLS-1-1-2017-01	<ul style="list-style-type: none"> <li>• ECDHE-ECDSA- -GCM- AES128 SHA256</li> <li>• ECDHE-RSA- AES128 -GCM- SHA256</li> </ul>

Política de seguridad	Cifrados
	<ul style="list-style-type: none"><li>• ECDHE-ECDSA- AES128 - SHA256</li><li>• ECDHE-RSA- - AES128 SHA256</li><li>• ECDHE-ECDSA- AES128 -SHA</li><li>• ECDHE-RSA- -SHA AES128</li><li>• ECDHE-ECDSA- AES256 -GCM- SHA384</li><li>• ECDHE-RSA- AES256 -GCM- SHA384</li><li>• ECDHE-ECDSA- AES256 - SHA384</li><li>• ECDHE-RSA- - AES256 SHA384</li><li>• ECDHE-ECDSA- AES256 -SHA</li><li>• ECDHE-RSA- -SHA AES256</li><li>• AES128-GCM- SHA256</li><li>• AES128-SHA256</li><li>• AES128-SHA</li><li>• AES256-GCM- SHA384</li><li>• AES256-SHA256</li><li>• AES256-SHA</li></ul>

Política de seguridad	Cifrados
ELBSecurityPolítica-2016-08	<ul style="list-style-type: none"><li>• ECDHE-ECDSA- -GCM- AES128 SHA256</li><li>• ECDHE-RSA- AES128 -GCM- SHA256</li><li>• ECDHE-ECDSA- AES128 - SHA256</li><li>• ECDHE-RSA- - AES128 SHA256</li><li>• ECDHE-ECDSA- AES128 -SHA</li><li>• ECDHE-RSA- -SHA AES128</li><li>• ECDHE-ECDSA- AES256 -GCM- SHA384</li><li>• ECDHE-RSA- AES256 -GCM- SHA384</li><li>• ECDHE-ECDSA- AES256 - SHA384</li><li>• ECDHE-RSA- - AES256 SHA384</li><li>• ECDHE-ECDSA- AES256 -SHA</li><li>• ECDHE-RSA- -SHA AES256</li><li>• AES128-GCM- SHA256</li><li>• AES128-SHA256</li><li>• AES128-SHA</li><li>• AES256-GCM- SHA384</li><li>• AES256-SHA256</li><li>• AES256-SHA</li></ul>

Política de seguridad	Cifrados
ELBSecurityPolítica-2015-05	<ul style="list-style-type: none"><li>• ECDHE-ECDSA- -GCM- AES128 SHA256</li><li>• ECDHE-RSA- AES128 -GCM- SHA256</li><li>• ECDHE-ECDSA- AES128 - SHA256</li><li>• ECDHE-RSA- - AES128 SHA256</li><li>• ECDHE-ECDSA- AES128 -SHA</li><li>• ECDHE-RSA- -SHA AES128</li><li>• ECDHE-ECDSA- AES256 -GCM- SHA384</li><li>• ECDHE-RSA- AES256 -GCM- SHA384</li><li>• ECDHE-ECDSA- AES256 - SHA384</li><li>• ECDHE-RSA- - AES256 SHA384</li><li>• ECDHE-ECDSA- AES256 -SHA</li><li>• ECDHE-RSA- -SHA AES256</li><li>• AES128-GCM- SHA256</li><li>• AES128-SHA256</li><li>• AES128-SHA</li><li>• AES256-GCM- SHA384</li><li>• AES256-SHA256</li><li>• AES256-SHA</li><li>• DES- -SHA CBC3</li></ul>

Política de seguridad	Cifrados
ELBSecurityPolítica-2015-03	<ul style="list-style-type: none"><li>• ECDHE-ECDSA- -GCM- AES128 SHA256</li><li>• ECDHE-RSA- AES128 -GCM- SHA256</li><li>• ECDHE-ECDSA- AES128 - SHA256</li><li>• ECDHE-RSA- - AES128 SHA256</li><li>• ECDHE-ECDSA- AES128 -SHA</li><li>• ECDHE-RSA- -SHA AES128</li><li>• ECDHE-ECDSA- AES256 -GCM- SHA384</li><li>• ECDHE-RSA- AES256 -GCM- SHA384</li><li>• ECDHE-ECDSA- AES256 - SHA384</li><li>• ECDHE-RSA- - AES256 SHA384</li><li>• ECDHE-ECDSA- AES256 -SHA</li><li>• ECDHE-RSA- -SHA AES256</li><li>• AES128-GCM- SHA256</li><li>• AES128-SHA256</li><li>• AES128-SHA</li><li>• AES256-GCM- SHA384</li><li>• AES256-SHA256</li><li>• AES256-SHA</li><li>• DHE-RSA- -SHA AES128</li><li>• DHE-DSS- AES128 -SHA</li><li>• DES- CBC3 -SHA</li></ul>

Política de seguridad	Cifrados
ELBSecurityPolítica-2015-02	<ul style="list-style-type: none"> <li>• ECDHE-ECDSA- -GCM- AES128 SHA256</li> <li>• ECDHE-RSA- AES128 -GCM- SHA256</li> <li>• ECDHE-ECDSA- AES128 - SHA256</li> <li>• ECDHE-RSA- - AES128 SHA256</li> <li>• ECDHE-ECDSA- AES128 -SHA</li> <li>• ECDHE-RSA- -SHA AES128</li> <li>• ECDHE-ECDSA- AES256 -GCM- SHA384</li> <li>• ECDHE-RSA- AES256 -GCM- SHA384</li> <li>• ECDHE-ECDSA- AES256 - SHA384</li> <li>• ECDHE-RSA- - AES256 SHA384</li> <li>• ECDHE-ECDSA- AES256 -SHA</li> <li>• ECDHE-RSA- -SHA AES256</li> <li>• AES128-GCM- SHA256</li> <li>• AES128-SHA256</li> <li>• AES128-SHA</li> <li>• AES256-GCM- SHA384</li> <li>• AES256-SHA256</li> <li>• AES256-SHA</li> <li>• DHE-RSA- -SHA AES128</li> <li>• DHE-DSS- AES128 -SHA</li> </ul>

## Políticas por cifrado

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

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL — 128-GCM - ECDHE-ECD SA-AES SHA256	<ul style="list-style-type: none"> <li>• ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>• ELBSecurityPolítica-TLS-1-1-2017-01</li> </ul>	c02b

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
IANA — TLS_ECDHE_ECDSA_CO_N_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	
OpenSSL — 128-GCM - ECDHE-RSA-AES SHA256  IANA — TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c02f
OpenSSL — 128- ECDHE-ECDSA-AES SHA256  IANA — TLS_ECDHE_ECDSA_CO_N_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c023
OpenSSL — 128- ECDHE-RSA-AES SHA256  IANA — TLS_ECDHE_RSA_CON_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c027

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
ECDHE-ECDSA-AESOpenSSL: 128-SHA  IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c009
ECDHE-RSA-AESOpenSSL: 128-SHA  IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c013
OpenSSL — 256-GCM - ECDHE-ECD SA-AES SHA384  IANA — TLS_ECDHE_ECDSA_CO N_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c02c
OpenSSL — 256-GCM - ECDHE-RSA- AES SHA384  IANA — TLS_ECDHE_RSA_CON_ AES_256_GCM_ SHA384	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c030

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL — 256- ECDHE-ECDSA-AES SHA384  IANA — TLS_ECDHE_ECDSA_CO_N_AES_256_CBC_SHA384	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c024
OpenSSL — 256- ECDHE-RSA-AES SHA384  IANA — TLS_ECDHE_RSA_CON_AES_256_CBC_SHA384	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c028
ECDHE-ECDSA-AES OpenSSL: 256-SHA  IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c014
ECDHE-RSA-AES OpenSSL: 256-SHA  IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	c00a

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL — -GCM- AES128 SHA256  IANA — TLS_RSA_CON_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	9c
OpenSSL — - AES128 SHA256  IANA — TLS_RSA_CON_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	3c
OpenSSL — SHA AES128  IANA: TLS_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	2f
OpenSSL — -GCM- AES256 SHA384  IANA — TLS_RSA_CON_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	9d

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL — - AES256 SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-2-2017-01</li> </ul>	3d
IANA — TLS_RSA_CON_AES_256_CBC_SHA256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	
OpenSSL — SHA AES256	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-TLS-1-1-2017-01</li> </ul>	35
IANA: TLS_RSA_WITH_AES_256_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2016-08</li> <li>ELBSecurityPolítica-2015-05</li> <li>ELBSecurityPolítica-2015-03</li> <li>ELBSecurityPolítica-2015-02</li> </ul>	
DHE-RSA-AESOpenSSL: 128-SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2015-03</li> </ul>	33
IANA: TLS_DHE_RSA_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2015-02</li> </ul>	
DHE-DSS-AESOpenSSL: 128-SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2015-03</li> </ul>	32
IANA: TLS_DHE_DSS_WITH_AES_128_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2015-02</li> </ul>	
OpenSSL — DES- -SHA CBC3	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2015-05</li> </ul>	0a
IANA: TLS_RSA_WITH_3DES_EDE_CBC_SHA	<ul style="list-style-type: none"> <li>ELBSecurityPolítica-2015-03</li> </ul>	

## Creación de un equilibrador de carga clásico con un oyente HTTPS

Un balanceador de cargas recibe las solicitudes de los clientes y las distribuye entre las EC2 instancias que están registradas en el balanceador de cargas.

Puede crear un equilibrador de carga capaz de detectar solicitudes en los puertos HTTP (80) y HTTPS (443). Si especifica que el oyente HTTPS debe enviar las solicitudes a las instancias a través del puerto 80, el equilibrador de carga terminará las solicitudes y la comunicación que tengan como destino instancias que no estén cifradas. Si el oyente HTTPS envía las solicitudes a las instancias a través del puerto 443, se cifrará la comunicación entre el equilibrador de carga y las instancias.

Si el equilibrador de carga utiliza una conexión cifrada para comunicarse con las instancias, es posible habilitar la autenticación de las instancias. De este modo, se asegura de que el equilibrador de carga solamente se comunique con una instancia si su clave pública coincide con la clave especificada en el equilibrador de carga para este fin.

Si desea obtener más información acerca de cómo incorporar un oyente HTTPS a un equilibrador de carga existente, consulte [Configuración de un oyente HTTPS para el equilibrador de carga clásico](#).

## Contenido

- [Requisitos previos](#)
- [Creación de un equilibrador de carga HTTPS a través de la consola](#)
- [Crea un balanceador de cargas HTTPS mediante el AWS CLI](#)

## Requisitos previos

Antes de empezar, asegúrese de que cumple los siguientes requisitos:

- Realice los pasos que se indican en [Recomendaciones para su VPC](#).
- Lanza las EC2 instancias que planeas registrar en tu balanceador de cargas. Los grupos de seguridad de estas instancias deben permitir el tráfico procedente del equilibrador de carga.
- Las EC2 instancias deben responder al objetivo de la comprobación de estado con un código de estado HTTP 200. Para obtener más información, consulte [Comprobación de estado de las instancias del Equilibrador de carga clásico](#).
- Si planeas habilitar la opción Keep-Alive en tus EC2 instancias, te recomendamos que establezcas la configuración de mantenerla activa como mínimo en la configuración de tiempo de espera de inactividad de tu balanceador de cargas. Si desea asegurarse de que el equilibrador de carga es el que se encarga de cerrar las conexiones con la instancia, asegúrese de que el valor definido en la instancia para el tiempo de keep-alive es mayor que el período de inactividad del equilibrador de carga. Para obtener más información, consulte [Configuración del tiempo de inactividad de conexión del equilibrador de carga clásico](#).

- Si crea un oyente seguro, debe implementar un certificado de servidor SSL en el equilibrador de carga. El equilibrador de carga utiliza el certificado para terminar y descifrar las solicitudes antes de enviarlas a las instancias. Si no dispone de un certificado SSL, puede crear uno. Para obtener más información, consulte [Certificados SSL/TLS para equilibradores de carga clásicos](#).

## Creación de un equilibrador de carga HTTPS a través de la consola

En este ejemplo, va a configurar dos oyentes para el equilibrador de carga. El primer oyente acepta solicitudes HTTP en el puerto 80 y las envía a las instancias a través del puerto 80 mediante HTTP. El segundo oyente acepta solicitudes HTTPS en el puerto 443 y las envía a las instancias mediante HTTP a través del puerto 80 (o mediante HTTPS a través del puerto 443 si desea configurar la autenticación de instancias backend).

Un oyente es un proceso que verifica solicitudes de conexión. El oyente se configura con un protocolo y un puerto para las conexiones frontend (entre el cliente y el equilibrador de carga) y otro protocolo y otro puerto para las conexiones backend (entre el equilibrador de carga y la instancia). Para obtener información sobre los puertos, los protocolos y las configuraciones de escucha compatibles con ELB, consulte. [Oyentes para el equilibrador de carga clásico](#)

Para crear un Equilibrador de carga clásico seguro 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 seleccionar la misma región que seleccionó para sus EC2 instancias.
3. En el panel de navegación, en Load Balancing (Equilibrio de carga), elija Load Balancers (Equilibradores de carga).
4. Elija Crear equilibrador de carga.
5. Amplíe la sección Equilibrador de carga clásico y, a continuación, seleccione Crear.
6. Configuración básica
  - a. En Nombre del equilibrador de carga, escriba un nombre para el equilibrador de carga. El nombre del equilibrador de carga clásico debe ser único en el conjunto de equilibradores de carga clásicos de la región, puede tener un máximo de 32 caracteres, solo puede contener caracteres alfanuméricos y guiones y no puede comenzar ni finalizar con un guion.
7. Asignación de redes
  - b. En Esquema, seleccione Orientado a Internet.

- a. En VPC, seleccione la misma VPC que haya seleccionado para las instancias.
- b. En Asignaciones, primero seleccione una zona de disponibilidad, y luego una subred pública de las subredes disponibles de esta. Solo puede seleccionar una subred por cada zona de disponibilidad. Para mejorar la disponibilidad del equilibrador de carga, seleccione más de una zona de disponibilidad y subred.

## 8. Grupos de seguridad

- En Grupos de seguridad, seleccione un grupo de seguridad existente que esté configurado para permitir el tráfico HTTP requerido en el puerto 80 y el tráfico HTTPS en el puerto 443.

Si no existe ninguno, puede crear un nuevo grupo de seguridad con las reglas necesarias.

## 9. Los oyentes y el enrutamiento

- a. Deje el oyente predeterminado con la configuración predeterminada y seleccione Agregar oyente.
- b. En Oyente, en el nuevo oyente, seleccione HTTPS como protocolo y el puerto se actualizará a 443. De manera predeterminada, Instancia utiliza el protocolo HTTP en el puerto 80.
- c. Si se necesita autenticación de backend, cambie el protocolo de Instancia a HTTPS. Esto también actualizará el puerto de Instancia a 443.

## 10. Configuración de oyente seguro

Si utiliza HTTPS o SSL con el oyente frontend, debe implementar un certificado SSL en el equilibrador de carga. El equilibrador de carga usará el certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de enviarlas a las instancias. Asimismo, debe especificar una política de seguridad. Elastic Load Balancing proporciona políticas de seguridad que tienen configuraciones de negociación SSL predefinidas, pero también puede crear su propia política de seguridad personalizada. Si la configuraste HTTPS/SSL en la conexión de back-end, puedes habilitar la autenticación de tus instancias.

- a. Para la política de seguridad, se recomienda utilizar siempre la política de seguridad predefinida más reciente o crear una personalizada. Consulte [Actualización de la configuración de negociación SSL](#).
- b. 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.
- c. (Opcional) Si ha configurado el oyente HTTPS para que se comunique con las instancias a través de una conexión cifrada, tiene la opción de configurar la autenticación de las instancias en Certificado de autenticación de backend.

 Note

Si no ve la sección Certificado de autenticación de backend, vuelva a Oyentes y enrutamiento y seleccione HTTPS como protocolo para Instancia.

- i. En Nombre de certificado, escriba el nombre del certificado de clave pública.
- ii. En Cuerpo del certificado (con codificación PEM), copie y pegue el contenido del certificado. El equilibrador de carga solamente se comunica con una instancia si su clave pública coincide con esta clave.
- iii. Para agregar otro certificado, seleccione Agregar nuevo certificado de backend. El límite es cinco.

## 11. Comprobaciones de estado

- a. En la sección Destino de ping, seleccione un Protocolo de ping y un Puerto de ping. EC2 Las instancias deben aceptar el tráfico del puerto ping especificado.
- b. En Puerto de ping, asegúrese de que el puerto sea 80.
- c. En Ruta de ping, sustituya el valor predeterminado por una barra diagonal (/). Esto le indica al ELB que envíe las solicitudes de verificación de estado a la página de inicio predeterminada del servidor web, por ejemplo. `index.html`

- d. En Configuración avanzada de comprobación de estado, utilice los valores predeterminados.

## 12. Instancias

- a. Seleccione Agregar instancias para que aparezca la pantalla de selección de instancias.
- b. En Instancias disponibles puede seleccionar entre las instancias actuales que estén disponibles para el equilibrador de carga, en función de la configuración de red seleccionada anteriormente.
- c. Cuando las selecciones le parezcan adecuadas, seleccione Confirmar para agregar las instancias que se deben registrar al equilibrador de carga.

## 13. Atributos

- En Habilitar equilibrio de carga entre zonas, Habilitar drenaje de conexiones y Tiempo de espera (intervalo de drenaje), mantenga los valores predeterminados.

## 14. Etiquetas del equilibrador de carga (opcionales)

- a. El campo Clave es obligatorio.
- b. El campo Valor es opcional.
- c. Para agregar otra etiqueta, seleccione Agregar nueva etiqueta y, a continuación, ingrese los valores en el campo Clave y, opcionalmente, en el campo Valor.
- d. Para eliminar una etiqueta existente, seleccione Eliminar junto a la etiqueta que desee eliminar.

## 15. Resumen y creación

- a. Si necesita cambiar alguna configuración, seleccione Editar junto a la configuración que sea necesario modificar.
- b. Cuando todas las configuraciones mostradas en el resumen le parezcan adecuadas, seleccione Crear equilibrador de carga para comenzar con la creación del equilibrador de carga.
- c. En la última página de creación, selecciona Ver balanceador de cargas para ver tu balanceador de cargas en la consola de Amazon EC2 .

## 16. Verificar

- a. Seleccione el nuevo equilibrador de carga.

- b. En la pestaña Instancias de destino, compruebe la columna Estado. Cuando al menos una de tus EC2 instancias esté en servicio, puedes probar el balanceador de carga.
- c. En la sección Detalles, copie el Nombre de DNS del equilibrador de carga, que debe parecerse a `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`.
- d. Pegue el Nombre de DNS del equilibrador de carga en el campo de direcciones de un navegador web conectado a la Internet pública. Si el equilibrador de carga funciona correctamente, verá la página predeterminada del servidor.

#### 17. Eliminar (opcional)

- a. Si tiene un registro CNAME para el dominio que señala al equilibrador de carga, apúntelo hacia una nueva ubicación y espere a que surta efecto el cambio de DNS antes de eliminar el equilibrador de carga.
- b. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
- c. Seleccione el equilibrador de carga.
- d. Seleccione Acciones, Eliminar equilibrador de carga.
- e. Cuando se le pida confirmación, escriba `confirm` y seleccione Eliminar.
- f. Tras eliminar un balanceador de cargas, las EC2 instancias que se registraron en él seguirán ejecutándose. Se le facturará cada hora parcial o completa que sigan ejecutándose. Cuando ya no necesites una EC2 instancia, puedes detenerla o cancelarla para evitar incurrir en cargos adicionales.

## Crea un balanceador de cargas HTTPS mediante el AWS CLI

Sigue las siguientes instrucciones para crear un HTTPS/SSL balanceador de cargas con AWS CLI

### Tareas

- [Paso 1: Configurar los oyentes](#)
- [Paso 2: Configurar la política de seguridad SSL](#)
- [Paso 3: Configurar la autenticación de instancias backend \(opcional\)](#)
- [Paso 4: Configurar comprobaciones de estado \(opcional\)](#)
- [Paso 5: Registrar las instancias EC2](#)
- [Paso 6: Comprobar las instancias](#)
- [Paso 7: Eliminar el equilibrador de carga \(opcional\)](#)

## Paso 1: Configurar los oyentes

Un oyente es un proceso que verifica solicitudes de conexión. El oyente se configura con un protocolo y un puerto para las conexiones frontend (entre el cliente y el equilibrador de carga) y otro protocolo y otro puerto para las conexiones backend (entre el equilibrador de carga y la instancia). Para obtener información sobre los puertos, los protocolos y las configuraciones de escucha compatibles con el ELB, consulte. [Oyentes para el equilibrador de carga clásico](#)

En este ejemplo, va a configurar dos oyentes del equilibrador de carga especificando los puertos y los protocolos que se van a usar para las conexiones frontend y backend. El primer oyente acepta solicitudes HTTP en el puerto 80 y envía solicitudes a las instancias a través del puerto 80 mediante HTTP. El segundo oyente acepta solicitudes HTTPS en el puerto 443 y envía solicitudes de las instancias mediante HTTP a través del puerto 80.

Como el segundo oyente utiliza HTTPS para la conexión frontend, debe implementar un certificado de servidor SSL en el equilibrador de carga. El equilibrador de carga utiliza el certificado para terminar y descifrar las solicitudes antes de enviarlas a las instancias.

Si desea configurar oyentes para su equilibrador de carga

1. Obtenga el nombre de recurso de Amazon (ARN) del certificado SSL. Por ejemplo:

ACM

```
arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

IAM

```
arn:aws:iam::123456789012:server-certificate/my-server-certificate
```

2. Utilice el siguiente [create-load-balancer](#) comando para configurar el equilibrador de carga con los dos oyentes:

```
aws elb create-load-balancer --load-balancer-name my-load-balancer --listeners  
  "Protocol=http,LoadBalancerPort=80,InstanceProtocol=http,InstancePort=80"  
  "Protocol=https,LoadBalancerPort=443,InstanceProtocol=http,InstancePort=80,SSLCertificateId=  
  --availability-zones us-west-2a
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "DNSName": "my-loadbalancer-012345678.us-west-2.elb.amazonaws.com"  
}
```

3. (Opcional) Usa el siguiente [describe-load-balancers](#) comando para ver los detalles del balanceador de cargas:

```
aws elb describe-load-balancers --load-balancer-name my-load-balancer
```

## Paso 2: Configurar la política de seguridad SSL

Puede seleccionar una de las políticas de seguridad predefinidas o crear su propia política de seguridad personalizada. De lo contrario, ELB configura el balanceador de cargas con la política de seguridad predefinida predeterminada, ELBSecurityPolicy-2016-08. Para obtener más información, consulte [Configuraciones de negociación SSL para el equilibrador de carga clásico](#).

Para comprobar si el equilibrador de carga está asociado a la política de seguridad predeterminada

Utilice el siguiente comando [describe-load-balancers](#):

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

A continuación, se muestra un ejemplo de respuesta. Observe que ELBSecurityPolicy-2016-08 está asociada con el equilibrador de carga en el puerto 443.

```
{  
  "LoadBalancerDescriptions": [  
    {  
      ...  
      "ListenerDescriptions": [  
        {  
          "Listener": {  
            "InstancePort": 80,  
            "SSLCertificateId": "ARN",  
            "LoadBalancerPort": 443,  
            "Protocol": "HTTPS",  
            "InstanceProtocol": "HTTP"  
          },  
          "PolicyNames": [  
            ...  
          ]  
        }  
      ]  
    }  
  ]  
}
```

```
        "ELBSecurityPolicy-2016-08"
    ],
},
{
    "Listener": {
        "InstancePort": 80,
        "LoadBalancerPort": 80,
        "Protocol": "HTTP",
        "InstanceProtocol": "HTTP"
    },
    "PolicyNames": []
}
],
...
}
]
```

Si lo prefiere, puede configurar la política de seguridad SSL del equilibrador de carga en lugar de utilizar la predeterminada.

(Opcional) Para utilizar una política de seguridad SSL predefinida

1. Utilice el siguiente [describe-load-balancer-policies](#) comando para enumerar los nombres de las políticas de seguridad predefinidas:

```
aws elb describe-load-balancer-policies
```

Para obtener información sobre la configuración de las políticas de seguridad predefinidas, consulte [Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos](#).

2. Utilice el siguiente [create-load-balancer-policy](#) comando para crear una política de negociación de SSL mediante una de las políticas de seguridad predefinidas que describió en el paso anterior:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType
--policy-attributes AttributeName=Reference-Security-
Policy,AttributeValue=predefined-policy
```

3. (Opcional) Utilice el siguiente [describe-load-balancer-policies](#) comando para comprobar que se ha creado la política:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-name my-SSLNegotiation-policy
```

La respuesta incluye la descripción de la política.

4. Use el siguiente comando [set-load-balancer-policies-of-listener](#) para habilitar la política en el puerto 443 del balanceador de carga:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

 Note

El comando `set-load-balancer-policies-of-listener` reemplaza el conjunto de políticas que se aplican actualmente en el puerto del equilibrador de carga especificado por el conjunto de políticas proporcionado. La lista `--policy-names` debería incluir todas las políticas que se van a habilitar. Si se omite una política que actualmente está habilitada, se desactivará.

5. (Opcional) Utilice el siguiente [describe-load-balancers](#) comando para comprobar que la política esté habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

En el siguiente ejemplo, se muestra que la política está habilitada en el puerto 443.

```
{
  "LoadBalancerDescriptions": [
    {
      ....
      "ListenerDescriptions": [
        {
          "Listener": {
            "InstancePort": 80,
            "SSLCertificateId": "ARN",
            "LoadBalancerPort": 443,
            "Protocol": "HTTPS",
            "InstanceProtocol": "HTTP"
          },
        ],
      ],
    }
  ],
}
```

```
        "PolicyNames": [
            "my-SSLNegotiation-policy"
        ],
        {
            "Listener": {
                "InstancePort": 80,
                "LoadBalancerPort": 80,
                "Protocol": "HTTP",
                "InstanceProtocol": "HTTP"
            },
            "PolicyNames": []
        }
    ],
    ...
}
]
```

Cuando cree una política de seguridad personalizada, debe habilitar al menos un protocolo y un cifrado. Los cifrados DSA y RSA son específicos del algoritmo de firma y se utilizan para crear el certificado SSL. Si ya tiene un certificado SSL, asegúrese de habilitar el cifrado que se usó para crearlo. El nombre de la política personalizada no debe comenzar por ELBSecurityPolicy- ni ELBSample-, ya que estos prefijos están reservados para los nombres de las políticas de seguridad predefinidas.

(Opcional) Para utilizar una política de seguridad SSL personalizada

1. Utilice el [create-load-balancer-policy](#) comando para crear una política de negociación de SSL mediante una política de seguridad personalizada. Por ejemplo:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy --policy-type-name
SSLNegotiationPolicyType
--policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
AttributeName=Protocol-TLSv1.1,AttributeValue=true
AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

2. (Opcional) Utilice el siguiente [describe-load-balancer-policies](#) comando para comprobar que se ha creado la política:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-name my-SSLNegotiation-policy
```

La respuesta incluye la descripción de la política.

3. Use el siguiente comando [set-load-balancer-policies-of-listener](#) para habilitar la política en el puerto 443 del balanceador de carga:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

 Note

El comando `set-load-balancer-policies-of-listener` reemplaza el conjunto de políticas que se aplican actualmente en el puerto del equilibrador de carga especificado por el conjunto de políticas proporcionado. La lista `--policy-names` debería incluir todas las políticas que se van a habilitar. Si se omite una política que actualmente está habilitada, se desactivará.

4. (Opcional) Utilice el siguiente [describe-load-balancers](#) comando para comprobar que la política esté habilitada:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

En el siguiente ejemplo, se muestra que la política está habilitada en el puerto 443.

```
{  
  "LoadBalancerDescriptions": [  
    {  
      ....  
      "ListenerDescriptions": [  
        {  
          "Listener": {  
            "InstancePort": 80,  
            "SSLCertificateId": "ARN",  
            "LoadBalancerPort": 443,  
            "Protocol": "HTTPS",  
            "InstanceProtocol": "HTTP"  
          },  
          ....  
        ]  
      ]  
    }  
  ]  
}
```

```
        "PolicyNames": [
            "my-SSLNegotiation-policy"
        ],
        {
            "Listener": {
                "InstancePort": 80,
                "LoadBalancerPort": 80,
                "Protocol": "HTTP",
                "InstanceProtocol": "HTTP"
            },
            "PolicyNames": []
        }
    ],
    ...
}
]
```

### Paso 3: Configurar la autenticación de instancias backend (opcional)

Si la configuras HTTPS/SSL en la conexión de back-end, puedes configurar de forma opcional la autenticación de tus instancias.

Cuando configure la autenticación de instancias backend, debe crear una política de clave pública. A continuación, utilizará esta política de clave pública para crear una política de autenticación de las instancias backend. Por último, configurará esta política de autenticación con el puerto de la instancia establecido para el protocolo HTTPS.

El equilibrador de carga solamente se comunica con una instancia si la clave pública que la instancia presenta al equilibrador de carga coincide con una clave pública de la política de autenticación del equilibrador de carga.

Para configurar la autenticación de instancias backend

1. Utilice el siguiente comando para recuperar la clave pública:

```
openssl x509 -in your X509 certificate PublicKey -pubkey -noout
```

2. Usa el siguiente [create-load-balancer-policy](#) comando para crear una política de clave pública:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-name my-PublicKey-policy \
--policy-type-name PublicKeyPolicyType --policy-attributes
AttributeName=PublicKey,AttributeValue=MIICiTCCAfICCCQD6m7oRw0uX0jANBhkqhkG9w
0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTA1dBMRAwDgYDVQQHEwdTZ
WF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC01BTSDb25zb2x1MRIw
EAYDVQQDEw1UZXN0Q21sYWMxHzAdBhkqhkG9w0BCQEWEG5vb251QGFtYXpvbi5
jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTEwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
MCVVMxCzAJBgNVBAgTA1dBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBb
WF6b24xFDASBgNVBAsTC01BTSDb25zb2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMx
HxAdBhkqhkG9w0BCQEWEG5vb251QGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySwtC2XADZ4nB+BLyGVI
k60CpiwsZ3G93vUEI03IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
ITx0USQv7c7ugFFDzQGBzZswY6786m86gpEIbb30hjZnzcvQaRHd1QWIIMm2nr
AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
KyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJI1J00zbhNYS5f6Guo
EDmFJ10ZxBHjJnyp3780D8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
3rrszlaEXAMPLE=
```

#### Note

Para especificar un valor de clave pública para --policy-attributes, elimine la primera y última línea de la clave pública (las líneas que contienen "-----BEGIN PUBLIC KEY-----" y "-----END PUBLIC KEY-----"). AWS CLI No acepta espacios en blanco--policy-attributes.

3. Use el siguiente [create-load-balancer-policy](#) comando para crear una política de autenticación de instancias de back-end mediante. **my-PublicKey-policy**

```
aws elb create-load-balancer-policy --load-balancer-name my-
loadbalancer --policy-name my-authentication-policy --policy-type-
name BackendServerAuthenticationPolicyType --policy-attributes
AttributeName=PublicKeyPolicyName,AttributeValue=my-PublicKey-policy
```

Si lo desea, también puede utilizar varias políticas de clave pública. El equilibrador de carga prueba todas las claves de una en una. Si la clave pública que presenta una instancia coincide con una de estas claves públicas, la instancia queda autenticada.

4. Usa el siguiente for-backend-server comando [set-load-balancer-policies](#): para establecer el puerto my-authentication-policy de la instancia para HTTPS. En este ejemplo, este puerto es el 443.

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 443 --policy-names my-authentication-policy
```

5. (Opcional) Usa el siguiente [describe-load-balancer-policies](#) comando para enumerar todas las políticas de tu balanceador de carga:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer
```

6. (Opcional) Usa el siguiente [describe-load-balancer-policies](#) comando para ver los detalles de la política:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --policy-names my-authentication-policy
```

#### Paso 4: Configurar comprobaciones de estado (opcional)

El ELB comprueba periódicamente el estado de cada EC2 instancia registrada en función de las comprobaciones de estado que hayas configurado. Si el ELB encuentra una instancia en mal estado, deja de enviar tráfico a la instancia y lo enruta a las instancias en buen estado. Para obtener más información, consulte [Comprobación de estado de las instancias del Equilibrador de carga clásico](#).

Al crear el balanceador de cargas, ELB usa la configuración predeterminada para las comprobaciones de estado. No obstante, si lo prefiere, puede modificar la configuración de las comprobaciones de estado del equilibrador de carga en lugar de utilizar la configuración predeterminada.

Para configurar las comprobaciones de estado de las instancias

Utilice el siguiente comando [configure-health-check](#):

```
aws elb configure-health-check --load-balancer-name my-loadbalancer --health-check Target=HTTP:80/ping,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

A continuación, se muestra un ejemplo de respuesta:

```
{
```

```
"HealthCheck": {  
    "HealthyThreshold": 2,  
    "Interval": 30,  
    "Target": "HTTP:80/ping",  
    "Timeout": 3,  
    "UnhealthyThreshold": 2  
}  
}
```

## Paso 5: Registrar las instancias EC2

Después de crear el balanceador de cargas, debes registrar tus EC2 instancias en el balanceador de cargas. Puedes seleccionar EC2 instancias de una sola zona de disponibilidad o de varias zonas de disponibilidad dentro de la misma región que el balanceador de cargas. Para obtener más información, consulte [Instancias registradas en el equilibrador de carga clásico](#).

Use el comando [register-instances-with-load-balancer](#) de la siguiente manera:

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --  
instances i-4f8cf126 i-0bb7ca62
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
    "Instances": [  
        {  
            "InstanceId": "i-4f8cf126"  
        },  
        {  
            "InstanceId": "i-0bb7ca62"  
        }  
    ]  
}
```

## Paso 6: Comprobar las instancias

El equilibrador de carga podrá usarse en cuanto una de las instancias registradas tenga el estado **InService**.

Para comprobar el estado de las EC2 instancias recién registradas, usa el siguiente comando: [describe-instance-health](#)

```
aws elb describe-instance-health --load-balancer-name my-loadbalancer --  
instances i-4f8cf126 i-0bb7ca62
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "InstanceStates": [  
    {  
      "InstanceId": "i-4f8cf126",  
      "ReasonCode": "N/A",  
      "State": "InService",  
      "Description": "N/A"  
    },  
    {  
      "InstanceId": "i-0bb7ca62",  
      "ReasonCode": "Instance",  
      "State": "OutOfService",  
      "Description": "Instance registration is still in progress"  
    }  
  ]  
}
```

Si el campo State de una instancia tiene el valor OutOfService, lo más probable es que las instancias estén aún en proceso de registro. Para obtener más información, consulte [Solución de problemas del equilibrador de carga clásico: registro de instancias](#).

Cuando al menos una de las instancias pasa al estado InService, se puede probar el equilibrador de carga. Para probar el equilibrador de carga, copie su nombre DNS y péguelo en el campo de direcciones de un navegador web que esté conectado a Internet. Si el equilibrador de carga está en ejecución, consulte la página predeterminada del servidor HTTP.

## Paso 7: Eliminar el equilibrador de carga (opcional)

Al eliminar un balanceador de cargas, se anula automáticamente el registro de las instancias asociadas EC2. Tan pronto como se elimina el equilibrador de carga, dejan de aplicarse cargos por él. Sin embargo, las EC2 instancias siguen ejecutándose y se siguen cobrando cargos.

Para eliminar el balanceador de cargas, usa el siguiente comando: [delete-load-balancer](#)

```
aws elb delete-load-balancer --load-balancer-name my-loadbalancer
```

Para detener EC2 las instancias, usa el comando [stop-instances](#). Para finalizar las EC2 instancias, usa el comando [terminate-instances](#).

## Configuración de un oyente HTTPS para el equilibrador de carga clásico

Un oyente es un proceso que verifica solicitudes de conexión. El oyente se configura con un protocolo y un puerto para las conexiones frontend (entre el cliente y el equilibrador de carga) y otro protocolo y otro puerto para las conexiones backend (entre el equilibrador de carga y la instancia). Para obtener información sobre los puertos, los protocolos y las configuraciones de escucha compatibles con ELB, consulte [Oyentes para el equilibrador de carga clásico](#)

Si tiene un equilibrador de carga con un oyente que acepta solicitudes HTTP en el puerto 80, puede agregar otro oyente que acepte solicitudes HTTPS en el puerto 443. Si especifica que el oyente HTTPS debe enviar las solicitudes a las instancias a través del puerto 80, el equilibrador de carga terminará las solicitudes SSL y la comunicación entre el equilibrador de carga y las instancias que no estén cifradas. Si el oyente HTTPS envía las solicitudes a las instancias a través del puerto 443, se cifrará la comunicación entre el equilibrador de carga y las instancias.

Si el equilibrador de carga utiliza una conexión cifrada para comunicarse con las instancias, tiene la opción de habilitar la autenticación de las instancias. De este modo, se asegura de que el equilibrador de carga solamente se comunique con una instancia si su clave pública coincide con la clave especificada en el equilibrador de carga para este fin.

Para obtener información sobre la creación de un nuevo oyente HTTPS, consulte [Creación de un equilibrador de carga clásico con un oyente HTTPS](#).

### Contenido

- [Requisitos previos](#)
- [Agregado de un oyente HTTPS a través de la consola](#)
- [Agrega un agente de escucha HTTPS mediante el AWS CLI](#)

### Requisitos previos

Para habilitar la compatibilidad con HTTPS en un oyente HTTPS, debe implementar un certificado de servidor SSL en el equilibrador de carga. El equilibrador de carga utiliza el certificado para terminar

y descifrar las solicitudes antes de enviarlas a las instancias. Si no dispone de un certificado SSL, puede crear uno. Para obtener más información, consulte [Certificados SSL/TLS para equilibradores de carga clásicos](#).

## Agregado de un oyente HTTPS a través de la consola

Puede agregar un oyente HTTPS a un equilibrador de carga existente.

Para agregar un oyente HTTPS al equilibrador de carga 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, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Oyentes, seleccione Administrar oyentes.
5. En la página Administrar oyentes, en la sección Oyentes, seleccione Agregar oyente.
6. En Protocolo del oyente, seleccione HTTPS.

**⚠ Important**

De manera predeterminada, el Protocolo de instancia es HTTP. Si desea configurar la autenticación de instancias backend, cambie el Protocolo de instancia a HTTPS.

7. Para la política de seguridad, se recomienda utilizar la política de seguridad predefinida más reciente. Si necesita utilizar otra política de seguridad predefinida o crear una política personalizada, consulte [Actualizar la configuración de negociación SSL](#).
8. En Certificado SSL predeterminado, seleccione Editar y, a continuación, realice una de las siguientes acciones:
  - Si creó o importó un certificado utilizando ACM AWS Certificate Manager, seleccione el certificado de la lista y, a continuación, seleccione Guardar cambios.

**ⓘ Note**

Esta opción solo está disponible en las regiones que admiten AWS Certificate Manager.

- Si ha importado un certificado mediante IAM, seleccione Desde IAM, seleccione el certificado en la lista y, a continuación, haga clic en Guardar cambios.

- Si tiene un certificado SSL para importar a ACM, seleccione Importar y A ACM. 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 (opcional), 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 lo acepten implícitamente.
  - Si tiene un certificado SSL para importar pero ACM no se admite en esta región, seleccione Importar y A IAM. En Nombre del certificado, escriba el 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 (opcional), 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 lo acepten implícitamente.
- Seleccione Save changes (Guardar cambios).
9. En Persistencia de cookie, el valor predeterminado es Desactivada. Para cambiarlo, seleccione Editar. Si selecciona Generada por el equilibrador de carga, se debe especificar un Periodo de vencimiento. Si selecciona Generada por la aplicación, se debe especificar un Nombre de cookie. Después de realizar la selección, seleccione Guardar cambios.
10. (Opcional) Seleccione Agregar oyente para agregar oyentes adicionales.
11. Seleccione Guardar cambios para agregar los oyentes que acaba de configurar.
12. (Opcional) Para configurar la autenticación de instancias de fondo para un balanceador de cargas existente, debes usar la AWS CLI o una API, ya que esta tarea no es compatible con la consola. Para obtener más información, consulte [Configurar la autenticación de instancias backend](#).

## Agrega un agente de escucha HTTPS mediante el AWS CLI

Puede agregar un oyente HTTPS a un equilibrador de carga existente.

Para añadir un agente de escucha HTTPS a tu balanceador de cargas mediante el AWS CLI

1. Obtenga el nombre de recurso de Amazon (ARN) del certificado SSL. Por ejemplo:

ACM

arn:aws:acm:*region*:123456789012:certificate/12345678-1234-1234-1234-123456789012

IAM

arn:aws:iam::123456789012:server-certificate/my-server-certificate

2. Usa el siguiente [create-load-balancer-listeners](#) comando para agregar un agente de escucha a tu balanceador de cargas que acepte solicitudes HTTPS en el puerto 443 y envíe las solicitudes a las instancias en el puerto 80 mediante HTTP:

```
aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --  
listeners  
  Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTP,InstancePort=80,SSLCertificateId=
```

Si desea configurar la autenticación de instancias backend, utilice el siguiente comando para agregar un oyente que acepte las solicitudes HTTPS en el puerto 443 y envíe las solicitudes a las instancias en el puerto 443 a través de HTTPS:

```
aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --  
listeners  
  Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTPS,InstancePort=443,SSLCertificate
```

3. (Opcional) Puedes usar el siguiente [describe-load-balancers](#) comando para ver los detalles actualizados de tu balanceador de cargas:

```
aws elb describe-load-balancers --load-balancer-name my-load-balancer
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerDescriptions": [  
    {  
      ...  
      "ListenerDescriptions": [  
        {  
          "Listener": {  
            "InstancePort": 80,  
            "SSLCertificateId": "ARN",  
            "LoadBalancerPort": 443,  
            "Protocol": "HTTP",  
            "SslCertificate": {  
              "ARN": "ARN",  
              "Status": "PENDING_ACTIVATION"  
            }  
          }  
        }  
      ]  
    }  
  ]  
}
```

```
        "Protocol": "HTTPS",
        "InstanceProtocol": "HTTP"
    },
    "PolicyNames": [
        "ELBSecurityPolicy-2016-08"
    ]
},
{
    "Listener": {
        "InstancePort": 80,
        "LoadBalancerPort": 80,
        "Protocol": "HTTP",
        "InstanceProtocol": "HTTP"
    },
    "PolicyNames": []
}
],
...
}
]
```

4. (Opcional) El oyente HTTPS se creó utilizando la política de seguridad predeterminada. Si desea especificar una política de seguridad predefinida diferente o una política de seguridad personalizada, utilice los comandos [create-load-balancer-policy](#) y [set-load-balancer-policies-of-listener](#). Para obtener más información, consulte [Actualizar la configuración de negociación de SSL mediante el AWS CLI](#).
5. (Opcional) Para configurar la autenticación de instancias de back-end, usa el comando [- set-load-balancer-policies for-backend-server](#) Para obtener más información, consulte [Configurar la autenticación de instancias backend](#).

## Reemplazo del certificado SSL del equilibrador de carga clásico

Si tiene un oyente HTTPS, cuando creó este oyente, implementó un certificado de servidor SSL en el equilibrador de carga. Cada certificado viene con un periodo de validez. No olvide renovar o sustituir el certificado antes de que finalice el periodo de validez.

Los certificados proporcionados AWS Certificate Manager e implementados en tu 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 . Cuando un certificado que está implementado en un equilibrador de carga se renueva, las nuevas solicitudes utilizan el certificado renovado.

Para sustituir un certificado, primero debe crear otro nuevo siguiendo los mismos pasos que utilizó para crear el certificado actual. A continuación, puede sustituir el certificado. Cuando un certificado que está implementado en un equilibrador de carga se reemplaza, las nuevas solicitudes utilizan el nuevo certificado.

Tenga en cuenta que la renovación o sustitución de un certificado no afecta a las solicitudes que ya se han recibido en un nodo del equilibrador de carga y que están pendiente de ser direccionadas a un destino con un estado correcto.

## Contenido

- [Reemplazo del certificado SSL a través de la consola](#)
- [Reemplazo del certificado SSL a través de la AWS CLI](#)

## Reemplazo del certificado SSL a través de la consola

Puede reemplazar el certificado implementado en el equilibrador de carga por un certificado proporcionado por ACM o un certificado cargado en IAM.

Para reemplazar el certificado SSL de un equilibrador de carga HTTPS 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 Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Oyentes, seleccione Administrar oyentes.
5. En la página Administrar oyentes, localice el oyente que desea actualizar, seleccione Editar en Certificado SSL predeterminado y realice una de las siguientes acciones:
  - Si creó o importó un certificado utilizando ACM AWS Certificate Manager, seleccione el certificado de la lista y, a continuación, seleccione Guardar cambios.

**Note**

Esta opción solo está disponible en las regiones que admiten AWS Certificate Manager.

- Si ha importado un certificado mediante IAM, seleccione Desde IAM, seleccione el certificado en la lista y, a continuación, haga clic en Guardar cambios.
- Si tiene un certificado SSL para importar a ACM, seleccione Importar y A ACM. 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 (opcional), 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 lo acepten implícitamente.
- Si tiene un certificado SSL para importar pero ACM no se admite en esta región, seleccione Importar y A IAM. En Nombre del certificado, escriba el 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 (opcional), 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 lo acepten implícitamente.
- Seleccione Save changes (Guardar cambios).

## Reemplazo del certificado SSL a través de la AWS CLI

Puede reemplazar el certificado implementado en el equilibrador de carga por un certificado proporcionado por ACM o un certificado cargado en IAM.

Para reemplazar un certificado SSL por un certificado proporcionado por ACM

1. Utilice el siguiente comando [request-certificate](#) para solicitar un nuevo certificado:

```
aws acm request-certificate --domain-name www.example.com
```

2. Use el siguiente comando [set-load-balancer-listener-ssl-certificate](#) para configurar el certificado:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-name my-load-balancer --load-balancer-port 443 --ssl-certificate-id arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Para reemplazar un certificado SSL por un certificado cargado en IAM

1. Si tiene un certificado SSL pero no lo ha cargado, consulte [Carga de un certificado de servidor](#) en la Guía del usuario de IAM.
2. Utilice el siguiente [get-server-certificate](#) comando para obtener el ARN del certificado:

```
aws iam get-server-certificate --server-certificate-name my-new-certificate
```

3. Use el siguiente comando [set-load-balancer-listener-ssl-certificate](#) para configurar el certificado:

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-name my-load-balancer --load-balancer-port 443 --ssl-certificate-id arn:aws:iam::123456789012:server-certificate/my-new-certificate
```

## Actualización de la configuración de la negociación SSL del equilibrador de carga clásico

ELB proporciona políticas de seguridad que tienen configuraciones de negociación de SSL predefinidas que se pueden utilizar para negociar las conexiones SSL entre los clientes y el balanceador de cargas. Si usa el HTTPS/SSL protocolo para su agente de escucha, puede usar una de las políticas de seguridad predefinidas o usar su propia política de seguridad personalizada.

Para obtener más información sobre las políticas de seguridad, consulte [Configuraciones de negociación SSL para el equilibrador de carga clásico](#). Para obtener información sobre las configuraciones de las políticas de seguridad proporcionadas por ELB, consulte [Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos](#)

Si crea un agente de HTTPS/SSL escucha sin asociar una política de seguridad, ELB asocia la política de seguridad predefinida predeterminada al equilibrador de ELBSecurityPolicy-2016-08 carga.

Si lo prefiere, puede crear una configuración personalizada. Le recomendamos encarecidamente que pruebe la política de seguridad antes de actualizar la configuración del equilibrador de carga.

En los siguientes ejemplos, se muestra cómo actualizar la configuración de negociación de SSL para un agente de escucha. HTTPS/SSL Tenga en cuenta que este cambio no afecta a las solicitudes recibidas por los nodos de equilibrador de carga y que están pendientes de ser direccionadas a una instancia correcta. La configuración actualizada comenzará a utilizarse con las nuevas solicitudes que se reciban.

## Contenido

- [Actualización de la configuración de negociación SSL a través de la consola](#)
- [Actualice la configuración de negociación de SSL mediante el AWS CLI](#)

## Actualización de la configuración de negociación SSL a través de la consola

De forma predeterminada, ELB asocia la última política predefinida a tu balanceador de cargas.

Cuando agregue una nueva política predefinida, le recomendamos que actualice el equilibrador de carga para que la utilice. También tiene la opción de seleccionar otra política de seguridad predefinida o crear una personalizada.

Para actualizar la configuración de negociación de SSL de un balanceador de HTTPS/SSL cargas 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 Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Oyentes, seleccione Administrar oyentes.
5. En la página Administrar oyentes, localice el oyente que desea actualizar, seleccione Editar en Política de seguridad y seleccione una política de seguridad mediante una de las siguientes opciones:
  - Mantén la política predeterminada, ELBSecurityPolicy-2016-08, y luego selecciona Guardar cambios.
  - Seleccione una política predefinida que no sea la predeterminada y haga clic en Guardar cambios.
  - Seleccione Personalizada y habilite al menos un protocolo y un cifrado, tal y como se indica a continuación:

- a. En SSL Protocols (Protocolos SSL), seleccione uno o varios protocolos para habilitarlos.
- b. Para SSL Options (Opciones SSL), seleccione Server Order Preference (Preferencia del orden del servidor) para usar el orden que aparece en [Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos](#) para la negociación SSL.
- c. En SSL Ciphers (Cifrados SSL), seleccione uno o varios cifrados para habilitarlos. Si ya tiene un certificado SSL, debe habilitar el cifrado que se usó para crearlo, ya que los cifrados DSA y RSA son específicos del algoritmo de firma.
- d. Seleccione Save changes (Guardar cambios).

## Actualice la configuración de negociación de SSL mediante el AWS CLI

Puede utilizar la política de seguridad predefinida `ELBSecurityPolicy-2016-08`, que es la predeterminada; una política de seguridad predefinida diferente, o una política de seguridad personalizada.

Para utilizar una política de seguridad SSL predefinida

1. Utilice el siguiente [describe-load-balancer-policies](#) comando para enumerar las políticas de seguridad predefinidas proporcionadas por ELB. La sintaxis que use dependerá del sistema operativo y del shell que esté utilizando.

Linux

```
aws elb describe-load-balancer-policies --query 'PolicyDescriptions[?PolicyType==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}' --output table
```

Windows

```
aws elb describe-load-balancer-policies --query "PolicyDescriptions[?PolicyType==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}" --output table
```

A continuación, se muestra un ejemplo de la salida:

```
-----  
|      DescribeLoadBalancerPolicies      |  
+-----+-----+
```

PolicyName
ELBSecurityPolicy-2016-08
ELBSecurityPolicy-TLS-1-2-2017-01
ELBSecurityPolicy-TLS-1-1-2017-01
ELBSecurityPolicy-2015-05
ELBSecurityPolicy-2015-03
ELBSecurityPolicy-2015-02
ELBSecurityPolicy-2014-10
ELBSecurityPolicy-2014-01
ELBSecurityPolicy-2011-08
ELBSample-ELBDefaultCipherPolicy
ELBSample-OpenSSLDefaultCipherPolicy

Para determinar qué cifrados están habilitadas en una política, utilice el siguiente comando:

```
aws elb describe-load-balancer-policies --policy-names ELBSecurityPolicy-2016-08 --  
output table
```

Para obtener información sobre la configuración de las políticas de seguridad predefinidas, consulte [Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos](#).

2. Utilice el [create-load-balancer-policy](#) comando para crear una política de negociación de SSL mediante una de las políticas de seguridad predefinidas que describió en el paso anterior. Por ejemplo, el comando siguiente utiliza la política de seguridad predefinida que se emplea de forma predeterminada:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer  
--policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType  
--policy-attributes AttributeName=Reference-Security-  
Policy,AttributeValue=ELBSecurityPolicy-2016-08
```

Si superas el límite de políticas para el balanceador de cargas, usa el [delete-load-balancer-policy](#) comando para eliminar las políticas no utilizadas.

3. (Opcional) Utilice el siguiente [describe-load-balancer-policies](#) comando para comprobar que se ha creado la política:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --  
policy-name my-SSLNegotiation-policy
```

La respuesta incluye la descripción de la política.

4. Use el siguiente comando [set-load-balancer-policies-of-listener](#) para habilitar la política en el puerto 443 del balanceador de carga:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-Loadbalancer
--load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

 Note

El comando `set-load-balancer-policies-of-listener` reemplaza el conjunto de políticas que se aplica actualmente en el puerto del equilibrador de carga especificado por el conjunto de políticas proporcionado. La lista `--policy-names` debería incluir todas las políticas que se van a habilitar. Si se omite una política que actualmente está habilitada, se desactivará.

5. (Opcional) Usa el siguiente [describe-load-balancers](#) comando para comprobar que la nueva política esté habilitada para el puerto del equilibrador de carga:

```
aws elb describe-load-balancers --load-balancer-name my-Loadbalancer
```

En la respuesta, puede verse que la política está habilitada en el puerto 443.

```
...
{
  "Listener": {
    "InstancePort": 443,
    "SSLCertificateId": "ARN",
    "LoadBalancerPort": 443,
    "Protocol": "HTTPS",
    "InstanceProtocol": "HTTPS"
  },
  "PolicyNames": [
    "my-SSLNegotiation-policy"
  ]
}
```

Cuando cree una política de seguridad personalizada, debe habilitar al menos un protocolo y un cifrado. Los cifrados DSA y RSA son específicos del algoritmo de firma y se utilizan para crear el certificado SSL. Si ya tiene un certificado SSL, asegúrese de habilitar el cifrado que se usó para crearlo. El nombre de la política personalizada no debe comenzar por ELBSecurityPolicy- ni ELBSample-, ya que estos prefijos están reservados para los nombres de las políticas de seguridad predefinidas.

Para utilizar una política de seguridad SSL personalizada

1. Utilice el [create-load-balancer-policy](#) comando para crear una política de negociación de SSL mediante una política de seguridad personalizada. Por ejemplo:

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy --policy-type-name
SSLNegotiationPolicyType
--policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
AttributeName=Protocol-TLSv1.1,AttributeValue=true
AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

Si superas el límite de políticas del balanceador de cargas, usa el [delete-load-balancer-policy](#) comando para eliminar las políticas no utilizadas.

2. (Opcional) Utilice el siguiente [describe-load-balancer-policies](#) comando para comprobar que se ha creado la política:

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

La respuesta incluye la descripción de la política.

3. Use el siguiente comando [set-load-balancer-policies-of-listener](#) para habilitar la política en el puerto 443 del balanceador de carga:

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
--load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

**Note**

El comando `set-load-balancer-policies-of-listener` reemplaza el conjunto de políticas que se aplica actualmente en el puerto del equilibrador de carga especificado por el conjunto de políticas proporcionado. La lista `--policy-names` debería incluir todas las políticas que se van a habilitar. Si se omite una política que actualmente está habilitada, se desactivará.

4. (Opcional) Usa el siguiente [`describe-load-balancers`](#) comando para comprobar que la nueva política esté habilitada para el puerto del equilibrador de carga:

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

En la respuesta, puede verse que la política está habilitada en el puerto 443.

```
...
{
  "Listener": {
    "InstancePort": 443,
    "SSLCertificateId": "ARN",
    "LoadBalancerPort": 443,
    "Protocol": "HTTPS",
    "InstanceProtocol": "HTTPS"
  },
  "PolicyNames": [
    "my-SSLNegotiation-policy"
  ]
}
...
```

# Instancias registradas en el equilibrador de carga clásico

Una vez que hayas creado tu Classic Load Balancer, debes registrar tus EC2 instancias en el balanceador de cargas. Puedes seleccionar EC2 instancias de una sola zona de disponibilidad o de varias zonas de disponibilidad dentro de la misma región que el balanceador de cargas. ELB realiza comprobaciones de estado de forma rutinaria en EC2 las instancias registradas y distribuye automáticamente las solicitudes entrantes al nombre DNS del balanceador de cargas entre las instancias registradas y en buen estado. EC2

## Contenido

- [Prácticas recomendadas para las instancias](#)
- [Recomendaciones para su VPC](#)
- [Registrar instancias con el Equilibrador de carga clásico](#)
- [Comprobación de estado de las instancias del Equilibrador de carga clásico](#)
- [Grupos de seguridad para las instancias del Equilibrador de carga clásico](#)
- [Red ACLs para las instancias de su Classic Load Balancer](#)

## Prácticas recomendadas para las instancias

- Debe asegurarse de que el equilibrador de carga pueda comunicarse con las instancias en el puerto del oyente y en el puerto de comprobación de estado. Para obtener más información, consulte [Configurar grupos de seguridad para el equilibrador de carga clásico](#). El grupo de seguridad de las instancias debe permitir el tráfico en ambas direcciones y en ambos puertos de cada subred del equilibrador de carga.
- Instale un servidor web, como Apache o Internet Information Services (IIS), en todas las instancias que tenga previsto registrar con su equilibrador de carga.
- Para los agentes de escucha HTTP y HTTPS, te recomendamos que habilites la opción Keep-Alive en tus EC2 instancias, que permite al balanceador de cargas reutilizar las conexiones a tus instancias para múltiples solicitudes de clientes. Esto reduce la carga del servidor web y mejora el rendimiento del equilibrador de carga. El tiempo de espera de keep-alive debe ser de 60 segundos como mínimo para garantizar que el equilibrador de carga es el encargado de cerrar la conexión con la instancia.
- ELB admite la detección de la unidad de transmisión máxima (MTU) de la ruta. Para garantizar que la detección de MTU de la ruta puede funcionar correctamente, debe asegurarse de que el

grupo de seguridad de la instancia permite los mensajes necesarios de fragmentación ICMP (tipo 3, 4). Para obtener más información, consulte [Path MTU Discovery](#) en la Guía del EC2 usuario de Amazon.

## Recomendaciones para su VPC

### Nube privada virtual (VPC)

A menos que haya creado la suya Cuenta de AWS antes de 2014, tiene una VPC predeterminada en cada región. Puede utilizar una VPC predeterminada para el equilibrador de carga o crear una nueva VPC. Para obtener más información, consulte la [Guía del usuario de Amazon VPC](#).

### Subredes del equilibrador de carga

Para garantizar que el equilibrador de carga puede adaptarse correctamente, asegúrese de que cada subred del equilibrador de carga tiene un bloque de CIDR con al menos una máscara de bits con el número /27 (por ejemplo, 10.0.0.0/27) y al menos ocho direcciones IP libres. El equilibrador de carga utiliza estas direcciones IP para establecer conexiones con las instancias y escalar horizontalmente cuando sea necesario. Si no hay suficientes direcciones IP, es posible que el equilibrador de carga no pueda escalar, lo que provocaría errores 503 debido a la falta de capacidad.

Cree una subred en cada zona de disponibilidad en la que desee lanzar instancias. En función de la aplicación, puede lanzar las instancias en subredes públicas, subredes privadas o en una combinación de subredes públicas y privadas. Una subred pública tiene una ruta hacia un gateway de Internet. Tenga en cuenta que, de forma predeterminada, VPCs tiene una subred pública por zona de disponibilidad.

Cuando crea un equilibrador de carga, debe agregarle una o varias subredes públicas. Si las instancias se encuentran en subredes privadas, cree subredes públicas en las mismas zonas de disponibilidad que las subredes que contienen las instancias y agregue estas subredes públicas al equilibrador de carga.

### Red ACLs

La red ACLs de la VPC debe permitir el tráfico en ambas direcciones en el puerto de escucha y en el puerto de comprobación de estado. Para obtener más información, consulte [Red ACLs para las instancias de su Classic Load Balancer](#).

## Registrar instancias con el Equilibrador de carga clásico

Al registrar una EC2 instancia, se añade a tu balanceador de cargas. El equilibrador de carga supervisa de forma continuada el estado de las instancias registradas en las zonas de disponibilidad habilitadas y direcciona las solicitudes a las instancias que tienen un estado correcto. Si la demanda de las instancias aumenta, puede registrar más instancias con el equilibrador de carga para hacerle frente.

Al anular el registro de una EC2 instancia, se elimina del balanceador de cargas. El equilibrador de carga deja de dirigir solicitudes a una instancia tan pronto como se anula su registro. Si disminuye la demanda o necesita realizar tareas de mantenimiento en las instancias, puede anular su registro en el equilibrador de carga. Cuando se anula el registro de una instancia, dicha instancia permanece en ejecución, aunque deja de recibir tráfico del equilibrador de carga. Si lo desea, puede volver a registrar la instancia con el equilibrador de carga cuando le venga bien.

Cuando cancelas el registro de una instancia, ELB espera a que se completen las solicitudes en curso si está habilitada la reducción de conexiones. Para obtener más información, consulte [Configuración de drenaje de conexiones en el equilibrador de carga clásico](#).

Si el equilibrador de carga está asociado a un grupo de escalado automático, las instancias del grupo se registran automáticamente con el equilibrador de carga. Si el equilibrador de carga no se puede desasociar de su grupo de escalado automático, se anula el registro de las instancias del grupo.

ELB registra la EC2 instancia en el balanceador de cargas mediante su dirección IP.

[EC2-VPC] Cuando registras una instancia con una interfaz de red elástica (ENI) conectada, el balanceador de carga enruta las solicitudes a la dirección IP principal de la interfaz principal (eth0) de la instancia.

### Contenido

- [Registro de una instancia](#)
- [Visualización de las instancias que se registran con el equilibrador de carga](#)
- [Determinación del equilibrador de carga para una instancia registrada](#)
- [Anulación del registro de una instancia](#)

## Registro de una instancia

Cuando esté preparado, registre la instancia con el equilibrador de carga. Si la instancia está en una zona de disponibilidad que está habilitada para el equilibrador de carga, la instancia estará lista para recibir tráfico del equilibrador de carga tan pronto como pase el número requerido de comprobaciones de estado.

Para registrar las instancias 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, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Instancias de destino, seleccione Administrar instancias.
5. En la página Administrar instancias, en la tabla Instancias disponibles, seleccione las instancias que desee registrar con el equilibrador de carga.
6. Asegúrese de que las instancias que deban registrarse aparezcan en la tabla Revisar instancias seleccionadas.
7. Seleccione Save changes (Guardar cambios).

Para registrar sus instancias mediante el AWS CLI

Usa el siguiente comando [register-instances-with-load-balancer](#):

```
aws elb register-instances-with-load-balancer --load-balancer-name my-Loadbalancer --  
instances i-4e05f721
```

A continuación, se incluye un ejemplo de respuesta donde se muestran las instancias registradas con el equilibrador de carga:

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-315b7e51"  
    },  
    {  
      "InstanceId": "i-4e05f721"  
    }  
  ]}
```

```
]  
}
```

## Visualización de las instancias que se registran con el equilibrador de carga

Usa el siguiente [describe-load-balancers](#) comando para enumerar las instancias registradas con el balanceador de cargas especificado:

```
aws elb describe-load-balancers --load-balancer-names my-Load-balancer --output text --  
query "LoadBalancerDescriptions[*].Instances[*].InstanceId"
```

A continuación, se muestra un ejemplo de la salida:

```
i-e905622e  
i-315b7e51  
i-4e05f721
```

## Determinación del equilibrador de carga para una instancia registrada

Usa el siguiente [describe-load-balancers](#) comando para obtener el nombre del balanceador de cargas en el que está registrada la instancia especificada:

```
aws elb describe-load-balancers --output text --query "LoadBalancerDescriptions[?  
Instances[?InstanceId=='i-e905622e']].[LoadBalancerName]"
```

A continuación, se muestra un ejemplo de la salida:

```
my-load-balancer
```

## Anulación del registro de una instancia

Puede anular el registro de una instancia del equilibrador de carga si ya no necesita su capacidad o si debe realizar tareas de mantenimiento.

Si el equilibrador de carga está asociado a un grupo de escalado automático, al desasociar la instancia del grupo también se anula su registro en el equilibrador de carga. Para obtener más información, consulte [Separar EC2 instancias de su grupo de Auto Scaling](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

Para anular el registro de las instancias 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, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Instancias de destino, seleccione Administrar instancias.
5. En la página Administrar instancias, en la tabla Instancias disponibles, anule la selección de las instancias cuyo registro con el equilibrador de carga deseé anular.
6. Asegúrese de que las instancias que cuyo registro se deba anular no aparezcan en la tabla Revisar instancias seleccionadas.
7. Seleccione Save changes (Guardar cambios).

Para anular el registro de sus instancias mediante el AWS CLI

Usa el siguiente comando [deregister-instances-from-load-balancer](#):

```
aws elb deregister-instances-from-load-balancer --load-balancer-name my-Loadbalancer --instances i-4e05f721
```

A continuación, se incluye un ejemplo de respuesta donde se muestran las instancias que siguen registradas con el equilibrador de carga:

```
{  
  "Instances": [  
    {  
      "InstanceId": "i-315b7e51"  
    }  
  ]  
}
```

## Comprobación de estado de las instancias del Equilibrador de carga clásico

El equilibrador de carga clásico envía periódicamente solicitudes a las instancias registradas para comprobar su estado. Estas pruebas se denominan comprobaciones de estado. El estado de las instancias que tienen un estado correcto cuando se realizan estas comprobaciones es **InService**. El estado de las instancias que tiene un estado que no es correcto cuando se realizan

estas comprobaciones es `OutOfService`. El equilibrador de carga realiza comprobaciones de estado en todas las instancias registradas, tanto en las que tienen un estado correcto como en las que no.

El equilibrador de carga dirige las solicitudes únicamente a las instancias que se encuentran en buen estado. Cuando el equilibrador de carga determina que una instancia tiene un estado que no es correcto, deja de dirigir solicitudes a esa instancia. El equilibrador de carga reanuda el direccionamiento de las solicitudes a esa instancia cuando esta vuelve a tener un estado correcto.

El balanceador de cargas comprueba el estado de las instancias registradas mediante la configuración de comprobación de estado predeterminada que proporciona ELB o una configuración de comprobación de estado que tú configures.

Si ha asociado el grupo de escalado automático con el equilibrador de carga clásico, puede utilizar la comprobación de estado del equilibrador de carga para determinar el estado de las instancias del grupo de escalado automático. De forma predeterminada, un grupo de escalado automático determina periódicamente el estado de cada instancia. Para obtener más información, consulte [Añadir comprobaciones de estado de ELB a su grupo de Auto Scaling](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

## Contenido

- [Configuración de la comprobación de estado](#)
- [Actualización de la configuración de la comprobación de estado](#)
- [Comprobación del estado de las instancias](#)
- [Solución de problemas de las comprobaciones de estado](#)

## Configuración de la comprobación de estado

Las configuraciones de estado contienen la información que un equilibrador de carga utiliza para determinar el estado de las instancias registradas. En la siguiente tabla se describen los campos de configuración de comprobación de estado.

Campo	Description (Descripción)
Protocolo	Protocolo que se utiliza para conectarse a la instancia. Los valores aceptados son: TCP, HTTP, HTTPS y SSL

Campo	Description (Descripción)
	<p>Valor predeterminado de la consola: HTTP</p> <p>Valor predeterminado de CLI/API: TCP</p>
Puerto	<p>Puerto que se utiliza para conectarse a la instancia; por ejemplo, un par <code>protocol:port</code> . Si el equilibrador de carga no puede conectarse a la instancia en el puerto especificado durante el período de espera de respuesta establecido, se considera que la instancia tiene un estado incorrecto.</p> <p>Protocolos: TCP, HTTP, HTTPS y SSL</p> <p>Rango de puertos: 1-65535</p> <p>Valor predeterminado de la consola: HTTP:80</p> <p>Valor predeterminado de CLI/API: TCP:80</p>
Ruta	<p>Destino de la solicitud HTTP o HTTPS.</p> <p>Se envía una solicitud HTTP o HTTPS GET a la instancia del puerto y la ruta. Si el equilibrador de carga recibe una respuesta distinta a "200 OK" durante el período de espera de respuesta, se considera que la instancia no tiene un estado correcto. Si la respuesta incluye un cuerpo, la aplicación debe establecer el encabezado Content-Length en un valor igual o mayor que cero o configurar Transfer-Encoding con un valor establecido en "chunked".</p> <p>Valor predeterminado: /index.html</p>

Campo	Description (Descripción)
Response Timeout	<p>Período de tiempo, en segundos, durante el que se va a esperar una respuesta de la comprobación de estado.</p> <p>Valores válidos: 2 - 60</p> <p>Valor predeterminado: 5</p>
HealthCheck Interval	<p>Período de tiempo, en segundos, que transcurre entre las comprobaciones de estado de una instancia individual.</p> <p>Valores válidos: 5 - 300</p> <p>Valor predeterminado: 30</p>
Unhealthy Threshold	<p>El número de comprobaciones de estado consecutivas fallidas que deben realizarse antes de declarar una EC2 instancia en mal estado.</p> <p>Valores válidos: 2-10</p> <p>Valor predeterminado: 2</p>
Healthy Threshold	<p>El número de comprobaciones de estado consecutivas que se han realizado correctamente antes de declarar una EC2 instancia en buen estado.</p> <p>Valores válidos: 2-10</p> <p>Valor predeterminado: 10</p>

El equilibrador de carga envía una solicitud de comprobación de estado a cada instancia registrada cada **Interval** segundos, utilizando el protocolo, la ruta y el puerto especificados. Cada solicitud de comprobación de estado es independiente y dura todo el intervalo. El tiempo que tarda la instancia en responder no afecta al intervalo de la siguiente comprobación de estado. Si las comprobaciones de estado superan los errores **UnhealthyThresholdCountconsecutivos**, el

balanceador de cargas deja la instancia fuera de servicio. Cuando las comprobaciones de estado superan las `HealthyThresholdCount` correctas consecutivas, el balanceador de cargas vuelve a poner la instancia en servicio.

Una HTTP/HTTPS comprobación de estado se realiza correctamente si la instancia devuelve un código de respuesta de 200 puntos dentro del intervalo de comprobación de estado. Del mismo modo, se considera que una comprobación de estado de TCP tiene éxito si la conexión TCP se ejecuta satisfactoriamente. Por último, se considera que una comprobación de estado de SSL tiene éxito si el protocolo de SSL se ejecuta satisfactoriamente.

## Actualización de la configuración de la comprobación de estado

Puede actualizar la configuración de la comprobación de estado de su equilibrador de carga en cualquier momento.

Para actualizar la configuración de la comprobación de estado de su equilibrador de carga 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, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la pestaña Health check, elija Edit.
5. En la página Editar configuración de comprobación de estado, en Comprobaciones de estado, actualice la configuración según sea necesario.
6. Cuando las selecciones le parezcan adecuadas, seleccione Guardar cambios.

Para actualizar la configuración del chequeo de estado del balanceador de cargas mediante el AWS CLI

Utilice el siguiente comando [configure-health-check](#):

```
aws elb configure-health-check --load-balancer-name my-load-balancer --health-check  
Target=HTTP:80/path,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

## Comprobación del estado de las instancias

Puede comprobar el estado de las instancias registradas.

Para comprobar el estado de las instancias 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, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir su página de detalles.
4. En la sección Detalles, Estado indica cuántas instancias están operativas.
5. En la pestaña Instancias de destino, en la tabla Instancias de destino, la columna Estado indica el estado concreto de cada instancia registrada.

Para comprobar el estado de sus instancias mediante el AWS CLI

Utilice el siguiente comando [describe-instance-health](#):

```
aws elb describe-instance-health --load-balancer-name my-load-balancer
```

## Solución de problemas de las comprobaciones de estado

Las instancias registradas pueden generar errores en la comprobación de estado del equilibrador de carga por diferentes motivos. Los motivos más comunes por los que no se supera una comprobación de estado son cuando las EC2 instancias cierran las conexiones con el balanceador de cargas o cuando se agota el tiempo de espera de la respuesta de las EC2 instancias. Si desea obtener más información sobre las causas posibles y los pasos que puede seguir para resolver los errores de comprobación de estado, consulte [Solución de problemas del equilibrador de carga clásico: comprobaciones de estado](#).

## Grupos de seguridad para las instancias del Equilibrador de carga clásico

Un grupo de seguridad funciona como un firewall y controla el tráfico permitido de entrada y salida de una o varias instancias. Al lanzar una EC2 instancia, puede asociar uno o más grupos de seguridad a la instancia. En cada grupo de seguridad, puede agregar una o varias reglas que permitan el tráfico. Puede modificar las reglas de un grupo de seguridad en cualquier momento; las nuevas reglas se aplican automáticamente a todas las instancias asociadas con el grupo de seguridad. Para obtener más información, consulte los [grupos EC2 de seguridad de Amazon](#) en la Guía del EC2 usuario de Amazon.

Los grupos de seguridad de las instancias deben permitir que estas se comuniquen con el equilibrador de carga. En la tabla siguiente, se muestran las reglas de entrada recomendadas.

origen	Protocolo	Rango de puertos	Comment
<i>load balancer security group</i>	TCP	<i>instance listener</i>	Permite el tráfico del equilibrador de carga en el puerto del oyente de la instancia
<i>load balancer security group</i>	TCP	<i>health check</i>	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.

## Red ACLs para las instancias de su Classic Load Balancer

Una lista de control de acceso (ACL) de red permite o deniega el tráfico entrante o saliente específico en el nivel de subred. Puede usar la ACL de red predeterminada para su VPC o puede crear una ACL de red personalizada para su VPC con reglas similares a las reglas de sus grupos de seguridad para agregar una capa de seguridad adicional a su VPC.

La lista de control de acceso (ACL) de red predeterminada de la VPC permite todo el tráfico de entrada y salida. Si creas una red personalizada ACLs, debes agregar reglas que permitan la comunicación entre el balanceador de cargas y las instancias.

Las reglas recomendadas para la subred de las instancias dependen de si la subred es pública o privada. Las siguientes reglas se han elaborado para subredes privadas. Si las instancias se encuentran en una subred pública, cambie el origen y el destino del CIDR de la VPC a  $0.0.0.0/0$ .

A continuación, se muestran las reglas de entrada recomendadas.

origen	Protocolo	Rango de puertos	Comment
--------	-----------	------------------	---------

origen	Protocolo	Rango de puertos	Comment
<i>VPC CIDR</i>	TCP	<i>instance listener</i>	Permite el tráfico de entrada procedente del CIDR de la VPC en el puerto de oyente de la instancia
<i>VPC CIDR</i>	TCP	<i>health check</i>	Permite el tráfico de entrada procedente del CIDR de la VPC en el puerto de comprobación de estado

A continuación, se muestran las reglas de salida recomendadas.

Destino	Protocolo	Rango de puertos	Comment
<i>VPC CIDR</i>	TCP	1024-65535	Permitir el tráfico de salida en el CIDR de la VPC a través de los puertos efímeros

# Monitoreo del Equilibrador de carga clásico

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 las instancias backend.

## CloudWatch métricas

ELB publica puntos de datos en Amazon CloudWatch sobre sus balanceadores de carga e instancias de back-end. CloudWatch le permite recuperar estadísticas sobre esos puntos de datos 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 tu Classic Load Balancer](#).

## Registros de acceso al ELB

Los registros de acceso a ELB capturan información detallada de las solicitudes realizadas a tu balanceador de cargas y la almacenan como archivos de registro en el bucket de Amazon S3 que especifiques. Cada registro contiene detalles como la hora de recepción de la solicitud, la dirección IP del cliente, las latencias, la ruta de solicitud y las respuestas de servidor. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar los problemas con las aplicaciones backend. Para obtener más información, consulte [Registros de acceso del Equilibrador de carga clásico](#).

## CloudTrail registros

AWS CloudTrail le permite realizar un seguimiento de las llamadas realizadas a la API de ELB por parte de su AWS cuenta o en su nombre. CloudTrail almacena la información en archivos de registro en el bucket de Amazon S3 que especifique. Puede utilizar estos archivos registro para monitorizar la actividad de los equilibradores de carga determinando las solicitudes que se han llevado a cabo, las direcciones IP de origen desde las que proceden las solicitudes, quién ha efectuado la solicitud, cuándo se ha realizado, etc. Para obtener más información, consulte [Registrar las llamadas a la API que se utilizan CloudTrail en ELB](#).

## CloudWatch métricas para tu Classic Load Balancer

ELB publica puntos de datos en Amazon CloudWatch para sus balanceadores de carga y sus instancias de back-end. CloudWatch le 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 supervisar el número total de EC2 instancias en buen estado de un balanceador de cargas durante un período de tiempo específico. 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, puedes 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 consideres un rango aceptable.

El ELB CloudWatch solo informa de las métricas cuando las solicitudes fluyen a través del balanceador de cargas. Si hay solicitudes que fluyen por el balanceador de cargas, ELB mide y envía sus métricas en 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.

Para obtener más información sobre Amazon CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

## Contenido

- [Métricas del Equilibrador de carga clásico](#)
- [Dimensiones de las métricas de los equilibradores de carga clásicos](#)
- [Estadísticas correspondientes a las métricas del Equilibrador de carga clásico](#)
- [Consulta CloudWatch las métricas de tu balanceador de cargas](#)

## Métricas del Equilibrador de carga clásico

El espacio de nombres de AWS/ELB incluye las siguientes métricas.

Métrica	Description (Descripción)
BackendConnectionErrors	El número de conexiones que no se establecieron correctamente entre el equilibrador de carga y las instancias registradas. Como el equilibrador de carga reintenta la conexión cuando hay errores, este recuento puede ser mayor que el número de solicitudes. Tenga en cuenta que este número incluye también todos los

Métrica	Description (Descripción)
	<p>errores de conexión relacionados con las comprobaciones de estado.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Sum. Tenga en cuenta que Average, Minimum y Maximum se registran para cada nodo del equilibrador de carga y no suelen tener ninguna utilidad. Sin embargo, la diferencia entre el mínimo y el máximo (o el valor máximo hasta el valor medio o el valor medio hasta el valor mínimo) puede resultar útil para determinar si un nodo del equilibrador de carga se comporta de manera anómala.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene dos instancias en us-west-2a y dos instancias en us-west-2b, y que los intentos de conectarse a una instancia en us-west-2a producen errores de conexión con el backend. La suma de us-west-2a incluye estos errores de conexión, pero no así la suma de us-west-2b. Por lo tanto, la suma del equilibrador de carga equivale a la suma de us-west-2a.</p>
DesyncMitigationMode_NonCompliant_Request_Count	<p>[Oyente HTTP] El número de solicitudes que no cumplen con RFC 7230.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Sum.</p>

Métrica	Description (Descripción)
HealthyHostCount	<p>El número de instancias en buen estado registradas con el equilibrador de carga. Una instancia recién registrada se considera que está en buen estado si supera la primera comprobación de estado. Si el equilibrio de carga entre zonas está habilitado, el número de instancias en buen estado para la dimensión <code>LoadBalancerName</code> se calcula en todas las zonas de disponibilidad. De lo contrario, se calcula para cada zona de disponibilidad.</p> <p>Criterios del informe: hay instancias registradas</p> <p>Estadísticas: las estadísticas más útiles son <code>Average</code> y <code>Maximum</code>. Estas estadísticas las determinan los nodos del equilibrador de carga. Tenga en cuenta que algunos nodos del equilibrador de carga podrían determinar que una instancia no está en buen estado durante un breve periodo y otros nodos determinar que sí está en buen estado.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene dos instancias en <code>us-west-2a</code> y dos instancias en <code>us-west-2b</code>; <code>us-west-2a</code> tiene una instancia en mal estado y <code>us-west-2b</code> tiene no tiene ninguna instancia en mal estado. Con la dimensión <code>AvailabilityZone</code>, se calcula una media de 1 instancia en buen estado y 1 instancia en mal estado en <code>us-west-2a</code>, y una media de 2 instancias en buen estado y 0 instancias en mal estado en <code>us-west-2b</code>.</p>

Métrica	Description (Descripción)
HTTPCode_Backend_2XX , HTTPCode_Backend_3XX , HTTPCode_Backend_4XX , HTTPCode_Backend_5XX	<p>[Oyente HTTP] El número de códigos de respuesta HTTP generados por las instancias registradas. Este número no incluye los códigos de respuesta generados por el equilibrador de carga.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Sum. Tenga en cuenta que Minimum, Maximum y Average tienen el valor de 1.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene dos instancias en us-west-2a y dos instancias en us-west-2b, y que las solicitudes enviadas a 1 instancia en us-west-2a producen respuestas HTTP 500. La suma de us-west-2a incluye estas respuestas de error, pero no así la suma de us-west-2b. Por lo tanto, la suma del equilibrador de carga equivale a la suma de us-west-2a.</p>
HTTPCode_ELB_4XX	<p>[Oyente HTTP] El número de códigos de error del cliente HTTP 4XX generados por el equilibrador de carga. Los errores del cliente se generan cuando una solicitud no tiene el formato correcto o está incompleta.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Sum. Tenga en cuenta que Minimum, Maximum y Average tienen el valor de 1.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene las regiones us-west-2a y us-west-2b habilitadas, y que las solicitudes del cliente incluyen una dirección URL con un formato incorrecto. Como resultado, los errores del cliente aumentarían probablemente en todas las zonas de disponibilidad. La suma del equilibrador de carga equivale a la suma de los valores de las zonas de disponibilidad.</p>

Métrica	Description (Descripción)
HTTPCode_ELB_5XX	<p>[Oyente HTTP] El número de códigos de error del servidor HTTP 5XX generados por el equilibrador de carga. Este número no incluye los códigos de respuesta generados por las instancias registradas. Esta métrica se registra si no hay ninguna instancia en buen estado registrada en el equilibrador de carga o si el número de solicitudes supera la capacidad de las instancias o del equilibrador de carga.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Sum. Tenga en cuenta que Minimum, Maximum y Average tienen el valor de 1.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene las regiones us-west-2a y us-west-2b habilitadas, y que las instancias de us-west-2a experimentan una alta latencia y tardan en responder a las solicitudes. Como resultado, la cola de sobrecarga de los nodos del equilibrador de carga en us-west-2a se llena y el cliente recibe un error 503. Si us-west-2b sigue respondiendo normalmente, la suma del equilibrador de carga equivale a la suma de us-west-2a.</p>

Métrica	Description (Descripción)
Latency	<p>[Oyente HTTP] Tiempo total, en segundos, transcurrido desde que el equilibrador de carga envió la solicitud a una instancia registrada hasta que esta comenzó a enviar los encabezados de la respuesta</p> <p>.</p> <p>[Oyente TCP] Tiempo total, en segundos, que tardó el equilibrador de carga en establecer una conexión correcta con una instancia registrada.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Average. Use Maximum para determinar si algunas solicitudes están tardando bastante más de la media. Tenga en cuenta que Minimum no suele ser útil.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene dos instancias en us-west-2a y dos instancias en us-west-2b, y que las solicitudes enviadas a 1 instancia en us-west-2a tienen una alta latencia. La media de us-west-2a tiene un valor mayor que la media de us-west-2b.</p>

Métrica	Description (Descripción)
RequestCount	<p>El número de solicitudes completadas o conexiones realizadas durante el intervalo especificado (1 o 5 minutos).</p> <p>[Oyente HTTP] El número de solicitudes recibidas y enrutas, incluidas las respuestas de error HTTP de las instancias registradas.</p> <p>[Oyente TCP] El número de conexiones realizadas en las instancias registradas.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Sum. Tenga en cuenta que Minimum, Maximum y Average devuelven 1.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene dos instancias en us-west-2a y dos instancias en us-west-2b, y que se envían 100 solicitudes al equilibrador de carga. Hay 60 solicitudes enviadas a us-west-2a, de las cuales cada instancia recibe 30, y hay 40 solicitudes enviadas a us-west-2b, de las cuales cada instancia recibe 20. Con la dimensión AvailabilityZone, se suman 60 solicitudes en us-west-2a y 40 solicitudes en us-west-2b. Con la dimensión LoadBalancerName, se suman 100 solicitudes.</p>

Métrica	Description (Descripción)
SpilloverCount	<p>El número total de solicitudes que se rechazaron porque la cola de sobrecarga está llena.</p> <p>[Oyente HTTP] El equilibrador de carga devuelve un código de error HTTP 503.</p> <p>[Oyente TCP] El equilibrador de carga cierra la conexión.</p> <p>Criterios del informe: hay un valor distinto de cero</p> <p>Estadísticas: la estadística más útil es Sum. Tenga en cuenta que Average, Minimum y Maximum se registran para cada nodo del equilibrador de carga y no suelen tener ninguna utilidad.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene las regiones us-west-2a y us-west-2b habilitadas, y que las instancias de us-west-2a experimentan una alta latencia y tardan en responder a las solicitudes. Como resultado, la cola de sobrecarga del nodo del equilibrador de carga en us-west-2a se llena, con lo que se supera la capacidad. Si us-west-2b sigue respondiendo normalmente, la suma del equilibrador de carga equivaldrá a la suma de us-west-2a.</p>

Métrica	Description (Descripción)
SurgeQueueLength	<p>Número total de solicitudes (oyente HTTP) o conexiones (oyente TCP) que están pendientes de direccionamiento a una instancia en buen estado. El tamaño máximo de la cola es 1 024. Las solicitudes o conexiones adicionales se rechazan cuando la cola está llena. Para obtener más información, consulte <a href="#">SpilloverCount</a> .</p> <p>Criterios del informe: hay un valor distinto de cero.</p> <p>Estadísticas: la estadística más útil es Maximum porque representa el valor máximo de solicitudes en cola. La estadística Average puede ser útil en combinación con Minimum y Maximum para determinar el intervalo de solicitudes en cola. Tenga en cuenta que Sum no es útil.</p> <p>Ejemplo: suponga que el equilibrador de carga tiene las regiones us-west-2a y us-west-2b habilitadas, y que las instancias de us-west-2a experimentan una alta latencia y tardan en responder a las solicitudes. Como resultado, la cola de sobrecarga de los nodos del equilibrador de carga en us-west-2a se llena y es probable que los clientes experimenten tiempos de respuesta mayores. Si esta situación continúa, el equilibrador de carga probablemente superará su capacidad (véase la métrica <a href="#">SpilloverCount</a> ). Si us-west-2b sigue respondiendo normalmente, el valor max del equilibrador de carga equivaldrá al valor max de us-west-2a.</p>

Métrica	Description (Descripción)
UnHealthyHostCount	<p>El número de instancias en mal estado registradas con el equilibrador de carga. Se considera que una instancia está en mal estado cuando supera el umbral de estado correcto configurado para las comprobaciones de estado. Se considera que una instancia en mal estado pasa a estar en buen estado cuando se mantiene en el umbral de estado correcto configurado para las comprobaciones de estado.</p> <p>Criterios del informe: hay instancias registradas</p> <p>Estadísticas: las estadísticas más útiles son Average y Minimum. Estas estadísticas las determinan los nodos del equilibrador de carga. Tenga en cuenta que algunos nodos del equilibrador de carga podrían determinar que una instancia no está en buen estado durante un breve periodo y otros nodos determinar que sí está en buen estado.</p> <p>Ejemplo: consulte <a href="#">HealthyHostCount</a> .</p>

Las siguientes métricas le permiten calcular los costos si migra un Equilibrador de carga clásico a un Equilibrador de carga de aplicación. Estas métricas están destinadas únicamente a fines informativos, no para su uso con CloudWatch alarmas. Tenga en cuenta que, si el Equilibrador de carga clásico tiene varios oyentes, estas métricas son la suma de todos ellos.

Estas estimaciones se basan en un equilibrador de carga con una regla predeterminada y un certificado con un tamaño de 2 K. Si usa un certificado con un tamaño de 4K o superior, le recomendamos que calcule los costos de la siguiente manera: cree un Equilibrador de carga de aplicación a partir del Equilibrador de carga clásico mediante la herramienta de migración y monitoree la métrica ConsumedLCUs para el Equilibrador de carga de aplicación. Para obtener más información, consulte [Migrar el Classic Load Balancer](#) en la Guía del usuario de Elastic Load Balancing.

Métrica	Description (Descripción)
EstimatedALBActiveConnectionCount	El número estimado de conexiones TCP simultáneas activas desde los clientes al equilibrador alanceador de carga y desde el equilibrador de carga a los destinos.
EstimatedALBConsumedLCUs	El número estimado de unidades de capacidad del equilibrador de carga (LCU) que utiliza un Equilibrador de carga de aplicación. Usted paga por la cantidad LCUs que utilice por hora. Para obtener más información, consulta los <a href="#">precios de ELB</a> .
EstimatedALBNewConnectionCount	El número estimado de conexiones TCP nuevas establecidas desde los clientes al equilibrador de carga y desde el equilibrador de carga a los destinos.
EstimatedProcessedBytes	El número estimado de bytes procesados por un Equilibrador de carga de aplicación.

## Dimensiones de las métricas de los equilibradores de carga clásicos

Para filtrar las métricas del Equilibrador de carga clásico, use las siguientes dimensiones.

Dimensión	Description (Descripción)
AvailabilityZone	Filtrá los datos de las métricas por la zona de disponibilidad especificada.
LoadBalancerName	Filtrá los datos de las métricas por el equilibrador de carga especificado.

## Estadísticas correspondientes a las métricas del Equilibrador de carga clásico

CloudWatch proporciona estadísticas basadas en los puntos de datos métricos publicados por el ELB. 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 name/value par que identifica de forma exclusiva una métrica. Por ejemplo, puedes 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 el mínimo y el máximo registrados en los nodos individuales del equilibrador de carga. Por ejemplo, supongamos que hay dos nodos del equilibrador de carga. Uno tiene la métrica **HealthyHostCount** con los siguientes valores: **Minimum**, 2; **Maximum**, 10; y **Average**, 6. En el otro nodo, los valores de la métrica **HealthyHostCount** son: **Minimum**, 1; **Maximum**, 5; y **Average**, 3. Por consiguiente, para el equilibrador de carga en su conjunto, **Minimum** es 1, **Maximum** es 10 y **Average** es aproximadamente 4.

La estadística **Sum** es el valor de la suma para todos los nodos del 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, tales como **RequestCount**, **HTTPCode\_ELB\_XXX**, **HTTPCode\_Backend\_XXX**, **BackendConnectionErrors** y **SpilloverCount**.

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.

Como alternativa, puedes ver las métricas de tu balanceador de carga mediante la CloudWatch consola.

Para consultar las métricas desde la consola de

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 para abrir su página de detalles.
4. Elija la pestaña Monitorización.
5. Para obtener una vista más amplia de una sola métrica, pase el cursor sobre su gráfico y, a continuación, seleccione el icono Maximize. Están disponibles las siguientes métricas:
  - Hosts en buen estado: `HealthyHostCount`
  - Hosts en mal estado: `UnHealthyHostCount`
  - Latencia media: `Latency`
  - Solicitudes: `RequestCount`
  - Errores de conexión backend — `BackendConnectionErrors`
  - Longitud de cola de oleada: `SurgeQueueLength`
  - Recuento de casos de superación de capacidad: `SpilloverCount`
  - HTTP 2 XXs — `HTTPCode_Backend_2XX`
  - HTTP 3 XXs — `HTTPCode_Backend_3XX`
  - HTTP 4 XXs — `HTTPCode_Backend_4XX`
  - HTTP 5 XXs — `HTTPCode_Backend_5XX`
  - ELB HTTP 4 — XXs `HTTPCode_ELB_4XX`
  - ELB HTTP 5 — XXs `HTTPCode_ELB_5XX`
  - Estimación de bytes procesados: `EstimatedProcessedBytes`
  - ALB consumido estimado: LCUs `EstimatedALBConsumedLCUs`
  - Número estimado de conexiones activas de ALB: `EstimatedALBActiveConnectionCount`

- Número estimado de nuevas conexiones de ALB: `EstimatedALBNewConnectionCount`

Para ver las métricas mediante la consola CloudWatch

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de ELB.
4. Realice una de las siguientes acciones:
  - Seleccione una dimensión de métrica para ver las métricas por equilibrador de carga, por zona de disponibilidad o para todos los equilibradores de carga.
  - Para ver una métrica en todas las dimensiones, escriba su nombre en el campo de búsqueda.
  - 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.

## Registros de acceso del Equilibrador de carga clásico

El ELB proporciona registros de acceso que recopilan información detallada sobre las solicitudes enviadas a tu balanceador de cargas. 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 función opcional del ELB que está deshabilitada de forma predeterminada. Tras habilitar los registros de acceso para el balanceador de cargas, ELB captura los registros y los almacena en el bucket de Amazon S3 que especifique. Puede deshabilitar el registro de acceso en cualquier momento.

Cada archivo de registro de acceso se cifra automáticamente mediante SSE-S3 antes de que se almacene en su bucket de S3 y se descifra al acceder al mismo. No es necesario que haga nada; el cifrado y descifrado se realizan de forma transparente. Cada archivo de registro se cifra con una clave única, que a su vez se cifra con una clave de KMS que se rota periódicamente. Para obtener

más información, consulte [Protección de datos mediante el cifrado del lado del servidor con las claves de cifrado administradas por Amazon S3 \(SSE-S3\)](#) en la Guía del usuario de Amazon S3.

Los registros de acceso no suponen ningún cargo adicional. Se le cobrarán los costes de almacenamiento de Amazon S3, pero no se le cobrará por el ancho de banda utilizado por ELB para enviar los archivos de registro a Amazon S3. Para obtener más información acerca de los costos de almacenamiento, consulte [Precios de Amazon S3](#).

## Contenido

- [Archivos de registro de acceso](#)
- [Entradas de los registros de acceso](#)
- [Procesamiento de registros de acceso](#)
- [Habilitación de los registros de acceso del Equilibrador de carga clásico](#)
- [Desactivación de los registros de acceso del Equilibrador de carga clásico](#)

## Archivos de registro de acceso

ELB publica un archivo de registro para cada nodo del balanceador de carga en el intervalo que especifique. Puede especificar un intervalo de publicación de 5 minutos o 60 minutos al habilitar el registro de acceso del equilibrador de carga. De forma predeterminada, ELB publica los registros con un intervalo de 60 minutos. Si el intervalo se establece en 5 minutos, los registros se publican a las 1:05, 1:10, 1:15 y así sucesivamente. El inicio de la entrega de registros se retrasa hasta 5 minutos si el intervalo es de 5 minutos y hasta 15 minutos si el intervalo es de 60 minutos. Puede modificar el intervalo de publicación en cualquier momento.

El equilibrador de carga puede entregar varios registros para el mismo periodo. Esto suele ocurrir si el sitio tiene mucho tráfico, varios nodos del equilibrador de carga y un intervalo breve de publicación de registros.

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

```
amzn-s3-demo-loadbalancer-logs[/logging-prefix]/AWSLogs/aws-account-id/  
elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_load-  
balancer-name_end-time_ip-address_random-string.log
```

aman-s3- demo-loadbalancer-logs

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 AWS de 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-name**

El nombre del equilibrador de carga.

**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 si el intervalo de publicación es de 5 minutos.

**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 "my-app":

```
s3://amzn-s3-demo-loadbalancer-logs/my-app/AWSLogs/123456789012/elasticloadbalancing/us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

A continuación, se muestra un ejemplo de nombre de archivo de registro sin un prefijo:

```
s3://amzn-s3-demo-loadbalancer-logs/AWSLogs/123456789012/elasticloadbalancing/us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

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 [Administración del ciclo de vida de los objetos](#) en la Guía del usuario de Amazon S3.

## Entradas de los registros de acceso

El ELB registra las solicitudes enviadas al balanceador de cargas, incluidas las solicitudes que nunca llegaron a las instancias de back-end. Por ejemplo, si un cliente envía una solicitud con un formato incorrecto o no hay ninguna instancia en buen estado para responder, la solicitud se registra igualmente.

### **Important**

El ELB registra las solicitudes haciendo el mejor esfuerzo posible. Recomendamos utilizar los registros de acceso para comprender la naturaleza de las solicitudes y no como una relación exhaustiva de todas las solicitudes.

## Sintaxis

Cada entrada de registro contiene los detalles de una única solicitud realizada al equilibrador de carga. Todos los campos de la entrada de registro están delimitados por espacios. Cada entrada del archivo registro presenta el siguiente formato:

```
timestamp elb client:port backend:port request_processing_time backend_processing_time
response_processing_time elb_status_code backend_status_code received_bytes sent_bytes
"request" "user_agent" ssl_cipher ssl_protocol
```

En la siguiente tabla se describen los campos de una entrada de registro de acceso.

Campo	Description (Descripción)
hora	Hora a la que el equilibrador de carga recibió la solicitud del cliente, en formato ISO 8601.
elb	El nombre del equilibrador de carga
client:port	Dirección IP y puerto del cliente solicitante.
backend:port	<p>Dirección IP y puerto de la instancia registrada que procesó esta solicitud.</p> <p>Si el equilibrador de carga no consigue enviar la solicitud a una instancia registrada o si una instancia cierra la conexión antes de haber podido enviar una respuesta, este valor se establece en -.</p> <p>Este valor también se puede establecer en - si la instancia registrada no responde antes de que se agote el tiempo de inactividad.</p>
request_processing_time	<p>[Oyente HTTP] Tiempo total, en segundos, transcurrido desde que el equilibrador de carga recibió la solicitud hasta que se la envió a una instancia registrada.</p> <p>[Oyente TCP] Tiempo total, en segundos, transcurrido desde que el equilibrador de carga aceptó una conexión de un cliente TCP/SSL hasta que envió el primer byte de datos a una instancia registrada.</p> <p>Este valor también se establece en -1 si el equilibrador de carga no consigue enviar la solicitud a una instancia registrada. Esto puede ocurrir si la instancia registrada cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto. Además, en el caso de los oyentes TCP, esto puede ocurrir si el cliente establece una conexión con el equilibrador de carga, pero no envía ningún dato.</p> <p>Este valor también se puede establecer en -1 si la instancia registrada no responde antes de que se agote el tiempo de inactividad.</p>

Campo	Description (Descripción)
backend_processing_time	<p>[Oyente HTTP] Tiempo total, en segundos, transcurrido desde que el equilibrador de carga envió la solicitud a una instancia registrada hasta que esta comenzó a enviar los encabezados de la respuesta.</p> <p>[Oyente TCP] Tiempo total, en segundos, que tardó el equilibrador de carga en establecer una conexión correcta con una instancia registrada.</p> <p>Este valor también se establece en -1 si el equilibrador de carga no consigue enviar la solicitud a una instancia registrada. Esto puede ocurrir si la instancia registrada cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto.</p> <p>Este valor también se puede establecer en -1 si la instancia registrada no responde antes de que se agote el tiempo de inactividad.</p>
response_processing_time	<p>[Oyente HTTP] Tiempo total (en segundos) transcurrido desde que el equilibrador de carga recibió el encabezado de respuesta de la instancia registrada 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.</p> <p>[Oyente TCP] Tiempo total (en segundos) transcurrido desde que el equilibrador de carga recibió el primer byte de la instancia registrada hasta que comenzó a enviar la respuesta al cliente.</p> <p>Este valor también se establece en -1 si el equilibrador de carga no consigue enviar la solicitud a una instancia registrada. Esto puede ocurrir si la instancia registrada cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto.</p> <p>Este valor también se puede establecer en -1 si la instancia registrada no responde antes de que se agote el tiempo de inactividad.</p>
elb_status_code	<p>[Oyente HTTP] Código de estado de la respuesta desde el equilibrador de carga.</p>

Campo	Description (Descripción)
backend_status_code	[Oyente HTTP] Código de estado de la respuesta desde la instancia registrada.
received_bytes	Tamaño de la solicitud, en bytes, recibida desde el cliente (solicitante).  [Oyente HTTP] El valor incluye el cuerpo de la solicitud, pero no los encabezados.  [Oyente TCP] El valor incluye el cuerpo de la solicitud y los encabezados.
sent_bytes	Tamaño de la respuesta, en bytes, enviada al cliente (solicitante).  [Oyente HTTP] El valor incluye el cuerpo de la respuesta, pero no los encabezados.  [Oyente TCP] El valor incluye el cuerpo de la solicitud y los encabezados.
solicitud	La línea de solicitud del cliente entre comillas dobles y registrada con el siguiente formato: Método HTTP + Protocolo://Encabezado de host:puerto + Ruta + 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.  [Oyente TCP] La dirección URL son tres guiones, separados entre sí por espacios y con un espacio al final ("---").
user_agent	[HTTP/HTTPS listener] A User-Agent string that identifies the client that originated the request. The string consists of one or more product identifiers, product/version. Si la cadena tiene más de 8 KB, se trunca.
ssl_cipher	[HTTPS/SSL listener] The SSL cipher. This value is recorded only if the incoming SSL/TLS la conexión se estableció después de una negociación exitosa. De lo contrario, el valor se establece en -.

Campo	Description (Descripción)
ssl_protocol	[HTTPS/SSL listener] The SSL protocol. This value is recorded only if the incoming SSL/TLS la conexión se estableció después de una negociación exitosa. De lo contrario, el valor se establece en -.

## Ejemplos

### Ejemplo de entrada HTTP

A continuación se muestra un ejemplo de entrada de registro para un oyente HTTP (del puerto 80 al puerto 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.000073
0.001048 0.000057 200 200 0 29 "GET http://www.example.com:80/ HTTP/1.1" "curl/7.38.0"
- -
```

### Ejemplo de entrada HTTPS

A continuación se muestra un ejemplo de entrada de registro para un oyente HTTPS (del puerto 443 al puerto 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80
0.000086 0.001048 0.001337 200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1"
"curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2
```

### Ejemplo de entrada TCP

A continuación se muestra un ejemplo de entrada de registro para un oyente TCP (del puerto 8080 al puerto 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001069
0.000028 0.000041 - - 82 305 "- - -" "-" - -
```

### Ejemplo de entrada SSL

A continuación se muestra un ejemplo de entrada de registro para un oyente SSL (del puerto 8443 al puerto 80):

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001065
0.000015 0.000023 - - 57 502 "-" "-" ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2
```

## Procesamiento de registros de acceso

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 interactivas que facilita el análisis de datos en Amazon S3 con SQL estándar. Para obtener más información, revise [Consulta de registros del Equilibrador de carga clásico](#) en la Guía del usuario de Amazon Athena.
- [Loggly](#)
- [Splunk](#)
- [Sumo Logic](#)

## Habilitación de los registros de acceso del Equilibrador de carga clásico

Para habilitar los registros de acceso del equilibrador de carga, debe especificar el nombre del bucket de Amazon S3 donde el equilibrador de carga almacenará los registros. También debes adjuntar una política de bucket a este bucket que otorgue al ELB permiso 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](#)
- [Resolución de problemas](#)

### Paso 1: Crear un bucket de S3

Al habilitar el registro de acceso, es preciso especificar un bucket de S3 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 [Cuotas, restricciones y limitaciones de bucket](#) 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

Su bucket de S3 debe tener una política de bucket que conceda permiso al ELB 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 utilizas un depósito existente que ya tiene una política adjunta, puedes añadir a la política la declaración relativa a los registros de acceso del ELB. 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.

## Política de bucket

Esta política otorga permisos al servicio de entrega de registros.

```
{  
  "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 la cuenta que contiene el equilibrador de carga en la ruta de recursos del ARN del bucket de S3. Esto garantiza que solo los equilibradores 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/*
```

[AWS GovCloud (US)] En el siguiente ejemplo, se utiliza la sintaxis ARN para las AWS GovCloud (US) Regions.

```
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 bucket de S3 es amzn-s3-demo-logging-bucket. No hay ninguna parte de prefijo en el ARN del bucket de S3.

```
arn:aws:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

[AWS GovCloud (US)] En el siguiente ejemplo, se utiliza la sintaxis ARN para las AWS GovCloud (US) Regions.

```
arn:aws-us-gov:s3:::amzn-s3-demo-logging-bucket/AWSLogs/123456789012/*
```

## Política de bucket heredada

Anteriormente, para las regiones disponibles antes de agosto de 2022, exigíamos una política que concediera permisos a una cuenta del ELB específica de la región. Esta política heredada sigue siendo compatible, pero le recomendamos que la sustituya por la política más reciente que se ha indicado anteriormente. Si lo prefiere, puede seguir utilizando la política de bucket heredada, que no se muestra aquí.

Como referencia, estas son las cuentas IDs del ELB para especificarlas. Principal Tenga en cuenta que las regiones que no figuran en esta lista no han admitido nunca la política de bucket heredada.

- 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
- AWS GovCloud (EEUU-Este) — 190560391635
- AWS GovCloud (US-Oeste) — 048591011584

## Prácticas recomendadas de seguridad

Para mejorar la seguridad, utilice un cubo S3 preciso. ARNs

- Utilice la ruta de recurso completa, no solo el ARN del bucket de S3.
- Incluya la parte del ID de cuenta del ARN del bucket de S3.
- No utilice caracteres comodín (\*) en la parte del ID de cuenta del ARN del bucket de S3.

Después de crear la política de bucket, utilice una interfaz de Amazon S3, como la consola o los AWS CLI comandos de Amazon S3, para adjuntar la política de bucket a su bucket de S3.

Para asociar su política de bucket a su bucket con la consola

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).

Para adjuntar su política de bucket a su bucket de S3 mediante el AWS CLI

Utilice el comando [put-bucket-policy](#). En este ejemplo, la política de bucket se ha guardado en el archivo .json especificado.

```
aws s3api put-bucket-policy \
--bucket amzn-s3-demo-bucket \
--policy file://access-log-policy.json
```

## 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 especificas un prefijo, no debe incluir la cadena "AWSLogs».

Configurar los registros de acceso para 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 Equilibrio de carga, elija 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 la página Editar atributos del equilibrador de carga, en la sección Monitoreo, haga lo siguiente:
  - a. Habilite los Registros de acceso.
  - b. 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://amzn-s3-demo-logging-bucket/logging-prefix*
    - URI sin un prefijo: *s3://amzn-s3-demo-logging-bucket*
  - c. En Intervalo de registro, mantenga 60 minutes - default.
  - d. Seleccione Save changes (Guardar cambios).

Para configurar los registros de acceso de su balanceador de carga mediante el AWS CLI

En primer lugar, cree un archivo.json que permita a ELB capturar y entregar los registros cada 60 minutos al depósito de S3 que creó para los registros:

{

```
"AccessLog": {  
    "Enabled": true,  
    "S3BucketName": "amzn-s3-demo-logging-bucket",  
    "EmitInterval": 60,  
    "S3BucketPrefix": "my-app"  
}  
}
```

A continuación, especifique el archivo.json en el [modify-load-balancer-attributes](#) comando de la siguiente manera:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes file://my-json-file.json
```

A continuación, se muestra un ejemplo de respuesta.

```
{  
    "LoadBalancerAttributes": {  
        "AccessLog": {  
            "Enabled": true,  
            "EmitInterval": 60,  
            "S3BucketName": "amzn-s3-demo-logging-bucket",  
            "S3BucketPrefix": "my-app"  
        }  
    },  
    "LoadBalancerName": "my-loadbalancer"  
}
```

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 hay un depósito nuevo con el mismo nombre y se ha creado la política de depósito requerida en un depósito Cuenta de AWS que no es de tu propiedad, ELB podría escribir los registros de acceso de tu balanceador de cargas en este nuevo depósito.

#### Paso 4: verificar los permisos del bucket

Una vez habilitados los registros de acceso para tu balanceador de cargas, ELB valida el bucket de S3 y crea un archivo de prueba para garantizar que la política del bucket especifique los permisos necesarios. Puede utilizar la consola de 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.

Para comprobar que ELB creó un archivo de prueba en su bucket de S3

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
2. Seleccione el nombre del bucket de S3 que especificó para los registros de acceso.
3. Vaya al archivo registro de prueba, ELBAccessLogFile. La ubicación depende de si utiliza un prefijo.
  - Ubicación con un prefijo:*amzn-s3-demo-loadbalancer-logs///logging-prefix/AWSLogs123456789012ELBAccessLogFile*
  - Ubicación sin prefijo:*amzn-s3-demo-loadbalancer-logs///AWSLogs123456789012ELBAccessLogFile*

## Resolución de problemas

Acceso denegado para el depósito:**bucket-name**. Compruebe el permiso de S3bucket

Si recibe este error, estas pueden ser causas posibles:

- La política del depósito no otorga al ELB permiso para escribir registros de acceso en el depósito. 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).

## Desactivación de los registros de acceso del Equilibrador de carga clásico

Se pueden deshabilitar los registros de acceso del equilibrador de carga en cualquier momento. Después de desactivar el registro de acceso, estos permanecerán en Amazon S3 hasta que los elimine. Para obtener más información, consulte [Uso de buckets de S3](#) en la Guía del usuario de Amazon S3.

Para deshabilitar los registros de acceso para 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 Equilibrio de carga, elija 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 la página Editar atributos del equilibrador de carga, en la sección Monitoreo, deshabilite Registros de acceso.

Para deshabilitar los registros de acceso mediante el AWS CLI

Use el siguiente [modify-load-balancer-attributes](#) comando para deshabilitar los registros de acceso:

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"AccessLog\":{\"Enabled\":false}}"
```

A continuación, se muestra un ejemplo de respuesta:

```
{  
  "LoadBalancerName": "my-loadbalancer",  
  "LoadBalancerAttributes": {  
    "AccessLog": {  
      "S3BucketName": "amzn-s3-demo-loadbalancer-logs",  
      "EmitInterval": 60,  
      "Enabled": false,  
      "S3BucketPrefix": "my-app"  
    }  
  }  
}
```

# Solución de problemas del equilibrador de carga clásico

En la siguiente lista, se enumeran recursos de solución de problemas que le resultarán útiles cuando trabaje con un equilibrador de carga clásico.

## errores de API

Error

[CertificateNotFound: Indefinido](#)

[OutofService: Se ha producido un error transitorio](#)

## Errores de HTTP

Error

[HTTP 400: BAD\\_REQUEST](#)

[HTTP 405: METHOD\\_NOT\\_ALLOWED](#)

[HTTP 408: Request timeout](#)

[HTTP 502: Bad gateway](#)

[HTTP 503: Service unavailable](#)

[HTTP 504: Gateway timeout](#)

## Métricas de código de respuesta

Métrica de código de respuesta

[HTTPCode\\_ELB\\_4XX](#)

[HTTPCode\\_ELB\\_5XX](#)

[HTTPCode\\_Backend\\_2xx](#)

## Métrica de código de respuesta

[HTTPCode\\_Backend\\_3xx](#)

[HTTPCode\\_Backend\\_4xx](#)

[HTTPCode\\_Backend\\_5xx](#)

## Problemas de comprobación de estado

### Problema

[Error en la página de destino de la comprobación de estado](#)

[Se ha agotado el tiempo de espera de conexión a las instancias](#)

[Se produce un error al autenticar la clave pública](#)

[La instancia no recibe tráfico desde el equilibrador de carga](#)

[Los puertos de la instancia no están abiertos](#)

[Las instancias de un grupo de escalado automático no superan la comprobación de estado de ELB](#)

## Problemas de conectividad

### Problema

[Los clientes no pueden conectarse a un equilibrador de carga orientado a internet](#)

[El equilibrador de carga no recibe las solicitudes enviadas a un dominio personalizado](#)

[Las solicitudes HTTPS que se envían al equilibrador de carga devuelven “NET: :ERR\\_CERT\\_COMMON\\_NAME\\_INVALID”](#)

## Problemas de registro de instancias

### Problema

[Registrar una EC2 instancia tarda demasiado](#)

[No se puede registrar una instancia lanzada desde una AMI pagada](#)

## Solución de problemas del equilibrador de carga clásico: errores de API

A continuación, se muestran los mensajes de error devueltos por la API de ELB, las posibles causas y los pasos que puede seguir para resolver los problemas.

### Mensajes de error

- [CertificateNotFound: Indefinido](#)
- [OutofService: Se ha producido un error transitorio](#)

### CertificateNotFound: Indefinido

Causa 1: se ha producido un retraso al propagar un certificado creado mediante la Consola de administración de AWS a todas las regiones. Si este retraso se produce, el mensaje de error aparece en el último paso del proceso de creación del equilibrador de carga.

Solución 1: espere aproximadamente 15 minutos y, a continuación, vuelva a intentarlo. Si el problema persiste, visite el [Centro de AWS Support](#) para obtener asistencia.

Causa 2: si utiliza la API AWS CLI o directamente, puede recibir este error si proporciona un nombre de recurso de Amazon (ARN) para un certificado que no existe.

Solución 2: utilice la acción AWS Identity and Access Management (IAM) [GetServerCertificate](#) para obtener el ARN del certificado y compruebe que ha proporcionado el valor correcto para el ARN.

### OutofService: Se ha producido un error transitorio

Causa: hay un problema interno transitorio en el servicio ELB o en la red subyacente. Este problema temporal también puede producirse cuando el ELB consulta el estado del balanceador de cargas y sus instancias registradas.

Solución: repita la llamada a la API. Si el problema persiste, visite el [Centro de AWS Support](#) para obtener asistencia.

## Solución de problemas del equilibrador de carga clásico: errores de HTTP

El método HTTP (también denominado verbo) especifica la acción que se va a realizar en el recurso que recibe una solicitud HTTP. Los métodos estándar para las solicitudes HTTP se definen en RFC 2616, [Method Definitions](#). Los métodos estándar son GET, POST, PUT, HEAD y OPTIONS. Algunas aplicaciones web requieren (y, en ocasiones, introducen) métodos que son extensiones de métodos HTTP/1.1. Algunos ejemplos habituales de métodos HTTP extendidos son PATCH, REPORT, MKCOL, PROPFIND, MOVE y LOCK. ELB acepta todos los métodos HTTP estándar y no estándar.

Las solicitudes y respuestas HTTP utilizan campos de encabezado para enviar información sobre los mensajes HTTP. Los campos de encabezados 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, [Message Headers](#). Para obtener más información, consulte [Encabezados HTTP y equilibradores de carga clásicos](#).

Cuando un equilibrador de carga recibe una solicitud HTTP, comprueba si hay solicitudes con un formato incorrecto y también la longitud del método. La longitud total del método de una solicitud HTTP a un equilibrador de carga no debe ser superior a 127 caracteres. Si la solicitud HTTP supera ambas comprobaciones, el balanceador de cargas envía la solicitud a la instancia. Si el campo de método de la solicitud no tiene el formato correcto, el equilibrador de carga responde con un error [HTTP 400: BAD\\_REQUEST](#). Si la longitud del método en la solicitud supera los 127 caracteres, el equilibrador de carga responde con un error [HTTP 405: METHOD\\_NOT\\_ALLOWED](#).

La EC2 instancia procesa una solicitud válida implementando el método en la solicitud y enviando una respuesta al cliente. Las instancias deben estar configuradas de tal forma que controlen los métodos admitidos y no admitidos.

A continuación se muestran los mensajes de error devueltos por el equilibrador de carga, sus posibles causas y las medidas que puede adoptar para resolver los problemas.

### Mensajes de error

- [HTTP 400: BAD\\_REQUEST](#)
- [HTTP 405: METHOD\\_NOT\\_ALLOWED](#)

- [HTTP 408: Request timeout](#)
- [HTTP 502: Bad gateway](#)
- [HTTP 503: Service unavailable](#)
- [HTTP 504: Gateway timeout](#)

## HTTP 400: BAD\_REQUEST

Descripción: indica que el cliente envió una solicitud incorrecta.

Causa 1: el cliente envió una solicitud incorrecta que no se ajusta a las especificaciones de HTTP. Por ejemplo, una solicitud no puede contener espacios en la URL.

Causa 2: el cliente utilizó el método HTTP CONNECT, que ELB no admite.

Solución: conéctese directamente a la instancia y capture los detalles de la solicitud del cliente. Revise los encabezados y la dirección URL para comprobar si el formato de las solicitudes es correcto. Compruebe que la solicitud cumple las especificaciones de HTTP. Verifique que se no se utilice HTTP CONNECT.

## HTTP 405: METHOD\_NOT\_ALLOWED

Descripción: indica que la longitud del método no es válida.

Causa: la longitud del método en el encabezado de la solicitud supera los 127 caracteres.

Solución: compruebe la longitud del método.

## HTTP 408: Request timeout

Descripción: indica que el cliente ha cancelado la solicitud o no ha podido enviar una solicitud completa.

Causa 1: una interrupción de la red o una construcción incorrecta de la solicitud; por ejemplo, el encabezado está parcialmente formado; el tamaño del contenido especificado no coincide con el tamaño del contenido real transmitido; etc.

Solución 1: revise el código que realiza la solicitud y pruebe a enviarlo directamente a las instancias registradas (o a un entorno de desarrollo/pruebas), donde disponga de mayor control para inspeccionar la solicitud en sí.

Causa 2: la conexión al cliente está cerrada (el equilibrador de carga no pudo enviar una respuesta).

Solución 2: verifique que el cliente no cierre la conexión antes de que se envíe la respuesta; para ello, utilice un rastreador de paquetes en la máquina que realiza la solicitud.

## HTTP 502: Bad gateway

Descripción: indica que el equilibrador de carga no ha podido analizar la respuesta enviada desde una instancia registrada.

Causa: el formato de la respuesta procedente de la instancia es incorrecto o puede haber un problema con el equilibrador de carga.

Solución: verifique que la respuesta enviada desde la instancia cumple las especificaciones de HTTP. Visite el [Centro de AWS Support](#) para obtener asistencia.

## HTTP 503: Service unavailable

Descripción: indica que el equilibrador de carga o las instancias registradas están provocando el error.

Causa 1: el equilibrador de carga no dispone de suficiente capacidad para controlar la solicitud.

Solución 1: el problema debería ser transitorio y no durar más de unos minutos. Si persiste, visite el [Centro de AWS Support](#) para obtener asistencia.

Causa 2: hay instancias no registradas.

Solución 2: registre al menos una instancia en cada zona de disponibilidad en la que el equilibrador de carga deba responder según su configuración. Verifíquelo consultando las HealthyHostCount métricas que aparecen en CloudWatch. Si no puede garantizar que haya una instancia registrada en cada zona de disponibilidad, recomendamos habilitar el balanceo de carga entre zonas. Para obtener más información, consulte [Configuración del equilibrio de carga entre zonas en el equilibrador de carga clásico](#).

Causa 3: no hay instancias con estado correcto.

Solución 3: asegúrese de que haya instancias en buen estado en cada zona de disponibilidad en la que el equilibrador de carga deba responder según su configuración. Para comprobarlo, consulte la métrica HealthyHostCount.

Causa 4: la cola de sobrecarga está llena.

Solución 4: asegúrese de que las instancias dispongan de capacidad suficiente para administrar la tasa de solicitudes. Para comprobarlo, consulte la métrica SpilloverCount.

## HTTP 504: Gateway timeout

Descripción: indica que el equilibrador de carga ha cerrado una conexión porque no se completó una solicitud dentro del tiempo de inactividad.

Causa 1: la aplicación tarda más en responder que el tiempo de inactividad configurado.

Solución 1: supervise las métricas HTTPCode\_ELB\_5XX y Latency. Si se produce un aumento de estas métricas, puede deberse a que la aplicación no responde antes de que transcurra el tiempo de inactividad. Para obtener más información sobre las solicitudes que están agotando el tiempo de espera, habilita los registros de acceso en el balanceador de cargas y revisa los 504 códigos de respuesta de los registros generados por el ELB. Si es necesario, puede aumentar su capacidad o aumentar el tiempo de inactividad configurado de manera que las operaciones largas (como la carga de archivos de gran tamaño) pueden completarse. Para obtener más información, consulta [Configuración del tiempo de inactividad de conexión del equilibrador de carga clásico](#) [Cómo solucionar problemas de alta latencia del ELB](#).

Causa 2: las instancias registradas cierran la conexión al ELB.

Solución 2: habilite la configuración de mantenimiento activo en sus EC2 instancias y asegúrese de que el tiempo de espera de mantenimiento activo sea mayor que el tiempo de espera de inactividad del balanceador de cargas.

## Solución de problemas del equilibrador de carga clásico: métricas de código de respuesta

El balanceador de cargas envía métricas a Amazon CloudWatch para los códigos de respuesta HTTP que se envían a los clientes e identifica el origen de los errores como el balanceador de cargas o las instancias registradas. Puedes usar las métricas devueltas por tu balanceador de cargas CloudWatch para solucionar problemas. Para obtener más información, consulte [CloudWatch métricas para tu Classic Load Balancer](#).

A continuación, se muestran las métricas del código de respuesta devueltas CloudWatch por tu balanceador de cargas, las posibles causas y las medidas que puedes tomar para resolver los problemas.

## Métricas de código de respuesta

- [HTTPCode\\_ELB\\_4XX](#)
- [HTTPCode\\_ELB\\_5XX](#)
- [HTTPCode\\_Backend\\_2xx](#)
- [HTTPCode\\_Backend\\_3xx](#)
- [HTTPCode\\_Backend\\_4xx](#)
- [HTTPCode\\_Backend\\_5xx](#)

### HTTPCode\_ELB\_4XX

Causa: una solicitud procedente del cliente cancelada o cuyo formato es incorrecto.

#### Soluciones

- Consulte [HTTP 400: BAD\\_REQUEST](#).
- Consulte [HTTP 405: METHOD\\_NOT\\_ALLOWED](#).
- Consulte [HTTP 408: Request timeout](#).

### HTTPCode\_ELB\_5XX

Causa: el equilibrador de carga o la instancia registrada es la causa del error, o bien el equilibrador de carga no puede analizar la respuesta.

#### Soluciones

- Consulte [HTTP 502: Bad gateway](#).
- Consulte [HTTP 503: Service unavailable](#).
- Consulte [HTTP 504: Gateway timeout](#).

### HTTPCode\_Backend\_2xx

Causa: una respuesta normal y satisfactoria procedente de las instancias registradas.

Solución: ninguna.

## HTTPCode\_Backend\_3xx

Causa: una respuesta de redirección enviada desde las instancias registradas.

Solución: consulte los registros de acceso o los registros de errores de la instancia para determinar la causa. Envíe las solicitudes directamente a la instancia (sin pasar por el equilibrador de carga) para ver las respuestas.

## HTTPCode\_Backend\_4xx

Causa: respuesta de error del cliente enviada desde las instancias registradas.

Solución: consulte los registros de acceso o los registros de errores de las instancias para determinar la causa. Envíe las solicitudes directamente a la instancia (sin pasar por el equilibrador de carga) para ver las respuestas.

 Note

Si el cliente cancela una solicitud HTTP iniciada con un encabezado `Transfer-Encoding: chunked`, existe un problema conocido que consiste en que el equilibrador de carga reenvía la solicitud a la instancia aunque el cliente haya cancelado la solicitud. Esto puede producir errores de backend.

## HTTPCode\_Backend\_5xx

Causa: respuesta de error del servidor enviada desde las instancias registradas.

Solución: consulte los registros de acceso o los registros de errores de las instancias para determinar la causa. Envíe las solicitudes directamente a la instancia (sin pasar por el equilibrador de carga) para ver las respuestas.

 Note

Si el cliente cancela una solicitud HTTP iniciada con un encabezado `Transfer-Encoding: chunked`, existe un problema conocido que consiste en que el equilibrador de carga reenvía la solicitud a la instancia aunque el cliente haya cancelado la solicitud. Esto puede producir errores de backend.

# Solución de problemas del equilibrador de carga clásico: comprobaciones de estado

El balanceador de cargas comprueba el estado de las instancias registradas mediante la configuración de comprobación de estado predeterminada que proporciona ELB o una configuración de comprobación de estado personalizada que tú especifiques. La configuración de comprobación de estado contiene información como el protocolo, el puerto de ping, la ruta de ping, el tiempo de espera de la respuesta y el intervalo de comprobación de estado. Se considera que una instancia se encuentra en buen estado si devuelve el código de respuesta 200 dentro del intervalo de comprobación de estado. Para obtener más información, consulte [Comprobación de estado de las instancias del Equilibrador de carga clásico](#).

Si el estado actual de algunas o todas las instancias es `OutOfService` y en el campo de descripción se muestra el mensaje `Instance has failed at least the Unhealthy Threshold number of health checks consecutively`, significa que las instancias no han superado la comprobación de estado del equilibrador de carga. A continuación se indican los problemas que pueden surgir, sus posibles causas y las medidas que debe adoptar para resolverlos.

## Problemas

- [Error en la página de destino de la comprobación de estado](#)
- [Se ha agotado el tiempo de espera de conexión a las instancias](#)
- [Se produce un error al autenticar la clave pública](#)
- [La instancia no recibe tráfico desde el equilibrador de carga](#)
- [Los puertos de la instancia no están abiertos](#)
- [Las instancias de un grupo de escalado automático no superan la comprobación de estado de ELB](#)

## Error en la página de destino de la comprobación de estado

Problema: una solicitud GET HTTP emitida a la instancia en el puerto de ping y la ruta de ping especificados (por ejemplo, `HTTP:80/index.html`) ha recibido un código de respuesta distinto de 200.

Causa 1: no se ha configurado ninguna página de destino en la instancia.

Solución 1: cree una página de destino (por ejemplo, `index.html`) en cada instancia registrada y especifique su ruta como ruta de ping.

Causa 2: no se ha establecido el valor del encabezado `Content-Length` de la respuesta.

Solución 2: si la respuesta incluye un cuerpo, establezca el encabezado Content-Length en un valor mayor o igual que cero, o bien establezca el valor de Transfer-Encoding en "chunked".

Causa 3: la aplicación no se ha configurado para recibir solicitudes desde el equilibrador de carga o para devolver el código de respuesta 200.

Solución 3: compruebe la aplicación de la instancia para investigar la causa.

## Se ha agotado el tiempo de espera de conexión a las instancias

Problema: las solicitudes de comprobación de estado del balanceador de cargas a las EC2 instancias se agotan o fallan de forma intermitente.

En primer lugar, conéctese directamente a la instancia para comprobar el problema. Recomendamos conectarse a la instancia desde la red mediante la dirección IP privada de la instancia.

Utilice el siguiente comando si se trata de una conexión TCP:

```
telnet private-IP-address-of-the-instance port
```

Utilice el siguiente comando si se trata de una conexión HTTP o HTTPS:

```
curl -I private-IP-address-of-the-instance:port/health-check-target-page
```

Si utilizas una HTTP/HTTPS conexión y recibes una respuesta distinta a 200, consulta [Error en la página de destino de la comprobación de estado](#). Si puede conectarse directamente a la instancia, compruebe lo siguiente:

Causa 1: la instancia no responde dentro del tiempo de espera de respuesta configurado.

Solución 1: ajuste la configuración del tiempo de espera de respuesta en la configuración de comprobación de estado del equilibrador de carga.

Causa 2: la instancia sufre una carga significativa y está tardando más en responder que el tiempo de espera de respuesta configurado.

Solución 2:

- compruebe el gráfico de monitorización por si la CPU está sobreutilizada. Para obtener más información, consulta [Obtener estadísticas de una EC2 instancia específica](#) en la Guía del EC2 usuario de Amazon.

- Compruebe el uso de otros recursos de la aplicación, como la memoria o los límites, conectándose a sus EC2 instancias.
- Si es necesario, agregue más instancias o habilite el escalado automático. Para obtener más información, consulte la [Guía del usuario EC2 de Amazon Auto Scaling](#).

Causa 3: si utiliza una conexión HTTP o HTTPS y la comprobación de estado se lleva a cabo en una página de destino especificada en el campo de la ruta de ping (por ejemplo, HTTP:80/index.html), puede que la página de destino esté tardando más en responder que el tiempo de espera configurado.

Solución 3: utilice una página de destino de comprobación de estado más sencilla o bien ajuste la configuración del intervalo de comprobación de estado.

## Se produce un error al autenticar la clave pública

Problema: se produce un error al autenticar la clave pública en un equilibrador de carga configurado para usar el protocolo HTTPS o SSL con la autenticación back-end habilitada.

Causa: la clave pública del certificado SSL no coincide con la clave pública configurada en el equilibrador de carga. Utilice el comando `s_client` para ver la lista de certificados de servidor en la cadena de certificados. Para obtener más información, consulte [s\\_client](#) en la documentación de OpenSSL.

Solución: es posible que deba actualizar el certificado SSL. Si el certificado SSL está vigente, pruebe a volver a instalarlo en el equilibrador de carga. Para obtener más información, consulte [Reemplazo del certificado SSL del equilibrador de carga clásico](#).

## La instancia no recibe tráfico desde el equilibrador de carga

Problema: el grupo de seguridad de la instancia bloquea el tráfico procedente del equilibrador de carga.

Realice una captura de paquetes en la instancia para comprobar el problema. Utilice el siguiente comando :

```
# tcpdump port health-check-port
```

Causa 1: el grupo de seguridad asociados con la instancia no permite el tráfico procedente del equilibrador de carga.

Solución 1: edite el grupo de seguridad de la instancia para permitir el tráfico procedente del equilibrador de carga. Agregue una regla para permitir todo el tráfico procedente del grupo de seguridad del equilibrador de carga.

Causa 2: el grupo de seguridad de su balanceador de carga no permite el tráfico a las EC2 instancias.

Solución 2: edita el grupo de seguridad del balanceador de cargas para permitir que el tráfico llegue a las subredes y las instancias. EC2

Para obtener más información acerca de la gestión de grupos de seguridad, consulte [Configurar grupos de seguridad para el equilibrador de carga clásico](#).

## Los puertos de la instancia no están abiertos

Problema: la comprobación de estado que el balanceador de cargas envía a la EC2 instancia está bloqueada por el puerto o un firewall.

Ejecute el comando siguiente para comprobar el problema:

```
netstat -ant
```

Causa: no está abierto el puerto de estado especificado o el puerto del oyente (si su configuración es distinta). Tanto el puerto especificado para la comprobación de estado como el puerto del oyente deben estar abiertos y a la escucha.

Solución: abra el puerto del oyente y el puerto especificado en la configuración de la comprobación de estado (si su configuración es distinta) en las instancias para recibir el tráfico procedente del equilibrador de carga.

## Las instancias de un grupo de escalado automático no superan la comprobación de estado de ELB

Problema: las instancias del grupo de escalado automático superan la comprobación de estado predeterminada de escalado automático pero no la de ELB.

Causa: Auto Scaling utiliza comprobaciones de EC2 estado para detectar problemas de hardware y software con las instancias, pero el balanceador de cargas realiza comprobaciones de estado enviando una solicitud a la instancia y esperando un código de respuesta de 200, o estableciendo una conexión TCP (para una verificación de estado basada en TCP) con la instancia.

Una instancia podría no superar la comprobación de estado de ELB si una aplicación que se ejecuta en la instancia tiene algún problema como consecuencia del cual el equilibrador de carga considera que la instancia se encuentra fuera de servicio. Esta instancia podría superar la comprobación de estado de Auto Scaling; no sería reemplazada por la política de Auto Scaling porque se considera en buen estado según la verificación de EC2 estado.

Solución: utilice la comprobación de estado de ELB para el grupo de escalado automático. Cuando se utiliza la comprobación de estado de ELB, escalado automático verifica los resultados de la comprobación de estado de la instancia y de la comprobación de estado de ELB para determinar el estado de las instancias. Para obtener más información, consulte [Añadir comprobaciones de estado de ELB a su grupo de Auto Scaling](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

## Solución de problemas del equilibrador de carga clásico: conectividad del cliente

### 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 el gateway de Internet de la nube virtual privada (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 de los puertos de escucha. Para obtener más información, consulte [Configurar grupos de seguridad para el equilibrador de carga clásico](#).

### 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.

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.

## Solución de problemas del equilibrador de carga clásico: registro de instancias

Al registrar una instancia en el equilibrador de carga, hay que realizar varios pasos antes de que el equilibrador de carga pueda comenzar a enviar solicitudes a esa instancia.

A continuación se indican los problemas que puede encontrar el balanceador de cargas al registrar EC2 las instancias, las posibles causas y las medidas que puede tomar para resolverlos.

### Problemas

- [Registrar una EC2 instancia tarda demasiado](#)

- [No se puede registrar una instancia lanzada desde una AMI pagada](#)

## Registrar una EC2 instancia tarda demasiado

Problema: EC2 las instancias registradas tardan más de lo esperado en estar en el InService estado.

Causa: puede que la instancia no haya superado la comprobación de estado. Después de llevar a cabo los pasos de registro de instancia por primera vez (puede tardar hasta aproximadamente 30 segundos), el equilibrador de carga comienza a enviar solicitudes de comprobación de estado. La instancia no adquiere el estado InService hasta que se supera una comprobación de estado.

Solución: consulte [Se ha agotado el tiempo de espera de conexión a las instancias.](#)

## No se puede registrar una instancia lanzada desde una AMI pagada

Problema: ELB no registra una instancia lanzada con una AMI de pago.

Causa: es posible que tus instancias se hayan lanzado con una AMI de pago de [Amazon DevPay](#).

Solución: ELB no admite el registro de instancias lanzadas con pagos AMIs de [Amazon DevPay](#). Ten en cuenta que puedes usar el servicio AMIs de pago de [AWS Marketplace](#). Si ya utilizas una AMI de pago AWS Marketplace y no puedes registrar una instancia lanzada desde esa AMI de pago, acude al [AWS Support Centro](#) para obtener ayuda.

# Cuotas del equilibrador de carga clásico

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.

Para ver las cuotas de los equilibradores de carga clásicos, abra la [consola de Service Quotas](#). En el panel de navegación, seleccione Servicios de AWS y elija Elastic Load Balancing. También puede usar el comando [describe-account-limits](#)(AWS CLI) para ELB.

Para solicitar un aumento de cuota, consulte [Solicitud de un aumento de cuota](#) en la Guía de usuario de Service Quotas.

Tu AWS cuenta tiene las siguientes cuotas relacionadas con los balanceadores de carga clásicos.

Name	Predeterminado	Ajustable
Equilibrador de carga clásico por región	20	<a href="#">Sí</a>
Oyentes para el Equilibrador de carga clásico	100	<a href="#">Sí</a>
Instancias registradas por Equilibrador de carga clásico	1 000	<a href="#">Sí</a>

# Historial de documentos para Equilibradores de carga clásicos

En la tabla siguiente, se describen las versiones de los equilibradores de carga clásicos.

Cambio	Descripción	Fecha
<a href="#"><u>Políticas de bucket para registros de acceso y registros de conexión</u></a>	Antes de esta versión, la política de bucket que utilizaba dependía de si la región estaba disponible antes o después de agosto de 2022. En esta versión, todas las regiones admiten la nueva política de bucket. Tenga en cuenta que la política de bucket heredada aún es compatible.	10 de septiembre de 2025
<a href="#"><u>Modo de mitigación de desincronización</u></a>	Se agregó compatibilidad con el modo de mitigación de desincronización. Para obtener más información, consulte <a href="#"><u>Configuración de modo de mitigación de desincronización del equilibrador de carga clásico</u></a> .	17 de agosto de 2020
<a href="#"><u>Equilibradores de carga clásicos</u></a>	Con la introducción de los equilibradores de carga de aplicaciones y los equilibradores de carga de red, los equilibradores de carga creados con la API 2016-06-01 se denominan equilibradores de carga clásicos. Para	11 de agosto de 2016

obtener más información sobre las diferencias entre estos tipos de balanceadores de carga, consulta las características del [ELB](#).

#### [Support for AWS Certificate Manager \(ACM\)](#)

Puede solicitar un SSL/TLS certificado a ACM e implementarlo en su balanceador de carga. Para obtener más información, consulte [SSL/TLS certificates for Classic Load Balancers](#).

21 de enero de 2016

#### [Compatibilidad con puertos adicionales](#)

Los equilibradores de carga pueden escuchar cualquier puerto comprendido entre el 1 y el 65535. Para obtener más información, consulte [Oyentes para el Equilibrador de carga clásico](#).

15 de septiembre de 2015

#### [Campos adicionales para entradas al registro de acceso](#)

Se han agregado los campos `user_agent` , `ssl_cipher` y `ssl_protocol` . Para obtener más información, consulte [Access log files](#).

18 de mayo de 2015

<u><a href="#">Compatibilidad con el etiquetado del equilibrador de carga</a></u>	A partir de esta versión, la CLI de ELB (CLI de ELB) se sustituyó por AWS Command Line Interface (AWS CLI), una herramienta unificada para administrar varios AWS servicios. Las nuevas características que se lancen después de la versión 1.0.35.0 de la ELB CLI (del 24 de julio de 2014) se incluirán únicamente en la AWS CLI . Si en la actualidad utiliza la ELB CLI, le recomendamos comenzar a usar la AWS CLI en su lugar. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface .	11 de agosto de 2014
<u><a href="#">Tiempo de inactividad de conexión</a></u>	Puede configurar el tiempo de inactividad de conexión del equilibrador de carga.	24 de julio de 2014
<u><a href="#">Compatibilidad con la concesión de acceso a los usuarios y grupos a equilibradores de carga específicos o acciones de API concretos</a></u>	Puede crear una política para conceder acceso a los usuarios y grupos a equilibradores de carga o acciones de API concretos.	12 de mayo de 2014

<a href="#"><u>Support para AWS CloudTrail</u></a>	Puede utilizarlo CloudTrail para capturar las llamadas a la API realizadas por usted o en su nombre Cuenta de AWS mediante la API del ELB Consola de administración de AWS, la CLI del ELB o la AWS CLI	4 de abril de 2014
<a href="#"><u>Drenaje de conexiones</u></a>	Se ha agregado información sobre el drenaje de conexiones. Con esta compatibilidad, puede permitir que el equilibrador de carga deje de enviar nuevas solicitudes a la instancia registrada mientras esta se encuentra en proceso de cancelación del registro o si se encuentra en mal estado, mientras las conexiones existentes se mantienen abiertas. Para obtener más información, consulte <a href="#"><u>Configuración del drenaje de conexiones en el Equilibrador de carga clásico</u></a> .	20 de marzo de 2014

Registros de acceso

Puede permitir que el equilibra dor de carga capture informaci ón detallada sobre las solicitud es enviadas al equilibrador de carga y almacenarla en un bucket de Amazon S3. Para obtener más informaci ón, consulte [Acceso a los registros de acceso del equilibrador de carga clásico](#).

Support para TLSv1.1-1.2

Se agregó información sobre la compatibilidad del protocolo TLSv1.1-1.2 para los balanceadores de carga configurados con agentes de escucha HTTPS/SSL. Con esta compatibilidad, Elastic Load Balancing también actualiza las configuraciones de negociación SSL predefinidas. Para obtener información sobre las configuraciones de negociación de SSL predefinidas actualizadas, consulte [Configuraciones de negociaci ón de SSL para los equilibra dores de carga clásicos](#). Para obtener información sobre la actualización de la configura ción de negociación de SSL actual, consulte [Update the SSL negotiation configuration of your Classic Load Balancer](#).

6 de marzo de 2014

<a href="#"><u>Equilibrio de carga entre zonas</u></a>	Se ha agregado información sobre cómo habilitar el balanceo de carga entre zonas en el equilibrador de carga. Para obtener más información, consulte <a href="#"><u>Configure cross-zone load balancing for your Classic Load Balancer</u></a> .	6 de noviembre de 2013
<a href="#"><u>Métricas adicionales CloudWatch</u></a>	Se agregó información sobre las métricas adicionales de Cloudwatch notificadas por ELB. Para obtener más información, consulte <a href="#"><u>CloudWatch las métricas de tu Classic Load Balancer</u></a> .	28 de octubre de 2013
<a href="#"><u>Compatibilidad con Proxy Protocol</u></a>	Se agregó información sobre la compatibilidad con el protocolo proxy para los平衡adores de carga configurados para TCP/SSL las conexiones. Para obtener más información, consulte <a href="#"><u>Proxy protocol header</u></a> .	30 de julio de 2013
<a href="#"><u>Compatibilidad con la conmutación por error de DNS</u></a>	Se ha agregado información sobre la configuración de conmutación por error de DNS de Amazon Route 53 para los equilibradores de carga. Para obtener más información, consulte <a href="#"><u>Using Amazon Route 53 DNS failover for your load balancer</u></a> .	3 de junio de 2013

<a href="#"><u>Soporte de consola para ver CloudWatch métricas y crear alarmas</u></a>	Se agregó información sobre la visualización de CloudWatch las métricas y la creación de alarmas para un balanceador de carga específico mediante la consola. Para obtener más información, consulte <a href="#"><u>CloudWatch las métricas de tu Classic Load Balancer</u></a> .	28 de marzo de 2013
<a href="#"><u>Support para registrar EC2 instancias en una VPC predeterminada</u></a>	Se ha añadido compatibilidad con EC2 las instancias lanzadas en una VPC predeterminada.	11 de marzo de 2013
<a href="#"><u>Equilibradores de carga internos</u></a>	A partir de esta versión, un equilibrador de carga de una nube virtual privada (VPC) puede estar expuesto a Internet o ser interno. Un equilibrador de carga interno tiene un nombre de DNS que se resuelve públicamente para generar direcciones IP privadas. Un equilibrador de carga expuesto a Internet tiene un nombre de DNS que se resuelve públicamente para generar direcciones IP públicas. Para obtener más información, consulte <a href="#"><u>Create an internal Classic Load Balancer</u></a> .	10 de junio de 2012

<a href="#"><u>Compatibilidad con la consola para administrar los oyentes, la configuración de cifrado y los certificados SSL</u></a>	Para obtener más información, consulte <a href="#"><u>Configure an HTTPS listener for your Classic Load Balancer</u></a> y <a href="#"><u>Replace the SSL certificate for your Classic Load Balancer</u></a> .	18 de mayo de 2012
<a href="#"><u>Support para ELB en Amazon VPC</u></a>	Se ha agregado compatibilidad con la creación de un equilibrador de carga en una nube virtual privada (VPC).	21 de noviembre de 2011
<a href="#"><u>Amazon CloudWatch</u></a>	Puede monitorizar su balanceador de carga mediante CloudWatch. Para obtener más información, consulte <a href="#"><u>CloudWatch las métricas de tu Classic Load Balancer</u></a> .	17 de octubre de 2011
<a href="#"><u>Características de seguridad adicionales</u></a>	Se pueden configurar cifrados SSL, SSL backend y la autenticación de servidor backend. Para obtener más información, consulte <a href="#"><u>Create a Classic Load Balancer with an HTTPS listener</u></a> .	30 de agosto de 2011
<a href="#"><u>Nombre de dominio de vértice de zona</u></a>	Para obtener más información, consulte <a href="#"><u>Configure a custom domain name for your Classic Load Balancer</u></a> .	24 de mayo de 2011

<a href="#"><u>Support for X-Forwarded-Proto and X-Forwarded-Port headers</u></a>	<p>El X-Forwarded-Proto encabezado indica el protocolo de la solicitud de origen y el X-Forwarded-Port encabezado indica el puerto de la solicitud de origen. La incorporación de estos encabezados a las solicitud es permite a los clientes determinar si una solicitud que entra en el equilibrador de carga está cifrada y el puerto concreto del equilibrador de carga en el que se ha recibido esa solicitud. Para obtener más información, consulte <a href="#"><u>HTTP headers and Classic Load Balancers</u></a>.</p>	27 de octubre de 2010
<a href="#"><u>Compatibilidad con HTTPS</u></a>	<p>Con esta versión, puede aprovechar el SSL/TLS protocolo para cifrar el tráfico y transferir el procesamiento SSL de la instancia de la aplicación al balanceador de cargas. Esta característica también ofrece administración centralizada de certificados de servidor SSL en el equilibra dor de carga, en lugar de tener que administrarlos en cada instancias de aplicación individual.</p>	14 de octubre de 2010
<a href="#"><u>Support for AWS Identity and Access Management (IAM)</u></a>	<p>Se ha agregado compatibi lidad con IAM.</p>	2 de septiembre de 2010

<a href="#"><u>Sesiones persistentes</u></a>	Para obtener más información, consulte <a href="#"><u>Configure sticky sessions for your Classic Load Balancer</u></a> .	7 de abril de 2010
<a href="#"><u>AWS SDK para Java</u></a>	Se ha agregado compatibilidad con SDK para Java.	22 de marzo de 2010
<a href="#"><u>AWS SDK para .NET</u></a>	Se agregó soporte para SDK para .NET	11 de noviembre de 2009
<a href="#"><u>Nuevo servicio</u></a>	Versión beta pública inicial de ELB.	18 de mayo de 2009

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