aws

Equilibradores de carga de aplicaciones

Elastic Load Balancing

Elastic Load Balancing: Equilibradores de carga de aplicaciones

Table of Contents

¿Qué es un Equilibrador de carga de aplicación? ... 1
Componentes del Equilibrador de carga de aplicación ... 1
Información general sobre Equilibrador de carga de aplicación ... 2
Ventajas de migrar desde un Equilibrador de carga clásico ... 3
Servicios de relacionados ... 4
Precios ... 5
Introducción ... 6
Antes de empezar ... 6
Paso 1: Configurar un grupo de destino ... 6
Paso 2: Elegir un tipo de equilibrador de carga ... 7
Paso 3: Configurar un equilibrador de carga y un oyente ... 8
Paso 4: Probar un equilibrador de carga ... 9
Paso 5: (Opcional) Eliminar el equilibrador de carga ... 9
Tutorial: Crear un Equilibrador de carga de aplicación con AWS CLI ... 11
Antes de empezar ... 11
Crear el equilibrador de carga ... 11
Adición de un oyente HTTPS ... 13
Agregar direccionamiento basado en rutas ... 14
Eliminar el equilibrador de carga ... 14
Equilibradores de carga ... 16
Subredes del equilibrador de carga ... 17
Subredes de zona de disponibilidad ... 17
Subredes de zona local ... 18
Subredes de Outpost ... 18
Grupos de seguridad del equilibrador de carga ... 20
Estado del equilibrador de carga ... 20
Atributos del equilibrador de carga ... 20
Tipo de dirección IP ... 23
Mapa de recursos del balanceador de carga ... 24
Componentes del mapa de recursos ... 25
Conexiones del balanceador de carga ... 26
Tiempo de inactividad de conexión ... 26
El tiempo de mantenimiento de la vida del cliente HTTP ... 27
Equilibrio de carga entre zonas ... 28

Protección contra eliminación ... 29
Modo de mitigación de desincronización ... 30
Conservación del encabezado del host ... 31
AWS WAF ... 34
Cree un equilibrador de carga ... 35
Paso 1: Configurar un grupo de destino ... 6
Paso 2: Registrar destinos ... 37
Paso 3: Configurar un equilibrador de carga y un oyente ... 38
Paso 4: Probar el equilibrador de carga ... 9
Actualización de zonas de disponibilidad ... 42
Actualización de grupos de seguridad ... 43
Reglas recomendadas ... 44
Actualizar los grupos de seguridad asociados ... 46
Actualizar el tipo de dirección ... 47
Actualización de etiquetas ... 48
Eliminar un equilibrador de carga de ... 49
Cambio de zona ... 50
Comenzar un cambio de zona ... 51
Actualizar un cambio de zona ... 52
Cancelar un cambio de zona ... 52
Oyentes y reglas ... 54
Configuración del oyente ... 54
Reglas del oyente ... 55
Reglas predeterminadas ... 56
Prioridad de las reglas ... 56
Acciones de las reglas ... 56
Condiciones de las reglas ... 56
Tipos de acción de regla ... 56
Acciones de respuesta fija ... 57
Acciones de reenvío ... 58
Acciones de redirección ... 61
Tipos de condición de las reglas ... 64
Condiciones de los encabezados HTTP ... 65
Condiciones de método de solicitud HTTP ... 66
Condiciones de host ... 66
Condiciones de ruta ... 68

Condiciones de cadena de consulta 69
Condiciones de dirección IP de origen 70
Crear un oyente HTTP 70
Requisitos previos 71
Agregar un oyente HTTP 71
Crear un oyente HTTPS 72
Certificados de SSL 73
Políticas de seguridad 75
Agregar un oyente HTTPS 100
Actualizar las reglas del oyente 102
Requisitos 102
Agregar una regla 103
Editar una regla 105
Reorganizar las reglas 106
Eliminar una regla 107
Actualizar un oyente HTTPS 108
Reemplazar el certificado predeterminado 108
Añadir certificados a la lista de certificados 109
Quitar certificados de la lista de certificados 110
Actualizar la política de seguridad 110
Utilice la autenticación TLS mutua 111
Antes de empezar 112
Encabezados HTTP 115
Configuración del TLS mutuo 117
Registros de conexión 123
Autenticar usuarios 123
Preparativos para usar un IdP compatible con OIDC 124
Preparación para usar Amazon Cognito 124
Prepárate para usar Amazon CloudFront 126
Configuración de la autenticación de usuarios 127
Flujo de autenticación 130
Codificación de las notificaciones de usuario y verificación de firmas 132
Tiempo de espera 136
Cierre de sesión de autenticación 137
Encabezados X-Forwarded 138
X-Forwarded-For 138

X-Forwarded-Proto ... 142
X-Forwarded-Port ... 142
Actualización de etiquetas ... 143
Actualizar las etiquetas de oyente ... 143
Actualizar las etiquetas de reglas ... 144
Eliminar un oyente ... 145
Grupos de destino ... 146
Configuración de enrutamiento ... 147
Tipo de destino ... 148
Tipo de dirección IP ... 149
Versión del protocolo ... 150
Destinos registrados ... 151
Atributos del grupo de destino ... 152
Los algoritmos de enrutamiento ... 154
Modifique el algoritmo de enrutamiento de un grupo objetivo ... 156
Pesos objetivo automáticos (ATW) ... 156
Detección de anomalías ... 157
Mitigación de anomalías ... 158
Retardo de anulación del registro ... 160
Modo de inicio lento ... 161
Crear un grupo de destino. ... 162
Configurar comprobaciones de estado ... 164
Configuración de comprobación de estado ... 165
Estado del destino ... 168
Códigos de motivo de comprobación de estado ... 170
Comprobación del estado de los destinos ... 171
Modificar la configuración de comprobación de estado de un grupo de destino ... 172
Balance de carga entre zonas ... 172
Deshabilitar el equilibrio de carga entre zonas ... 174
Habilitar equilibrio de carga entre zonas ... 175
Estado del grupo de destino ... 176
Acciones en mal estado ... 176
Requisitos y consideraciones ... 176
Supervisión ... 177
Ejemplo ... 177
Modificación de la configuración de estado de grupo de destino ... 179

Uso de la conmutación por error de DNS de Route 53 para el equilibrador de carga 180
Cómo registrar destinos 181
Grupos de seguridad de destino 182
Subredes compartidas 182
Registro o anulación del registro de destinos 182
Sesiones persistentes 185
Persistencia en función de la duración 187
Persistencia en función de la aplicación 189
Funciones de Lambda como destino 192
Preparar la función de Lambda 193
Creación de un grupo de destino para la función de Lambda 185
Recibir eventos del equilibrador de carga 195
Responder al equilibrador de carga 196
Encabezados de varios valores 197
Deshabilitar las comprobaciones de estado 199
Anular el registro de la función de Lambda 201
Actualización de etiquetas 201
Eliminación de un grupo de destino 202
Monitorización de los equilibradores de carga 204
CloudWatch métricas 205
Métricas del Equilibrador de carga de aplicación 206
Dimensiones de las métricas de los equilibradores de carga de aplicaciones 225
Estadísticas para métricas del Equilibrador de carga de aplicación 226
Consulta CloudWatch las métricas de tu balanceador de cargas 227
Registros de acceso 230
Archivos de registro de acceso 230
Entradas de los registros de acceso 232
Ejemplo de entradas de registro 246
Procesamiento de archivos de registro de acceso 249
Habilitación de registros de acceso 249
Desactivación de los registros de acceso 257
Registros de conexión 258
Archivos de registro de conexiones 258
Entradas de registro de conexión 260
Ejemplo de entradas de registro 264
Procesamiento de archivos de registro de conexiones 264

Habilite los registros de conexión 265
Inhabilite los registros de conexión 271
Rastreo de solicitudes 272
Sintaxis 272
Limitaciones 273
CloudTrail registros 273
Información sobre Elastic Load Balancing en CloudTrail 274
Descripción de las entradas del archivo de registros de Elastic Load Balancing 275
Solución de problemas de equilibradores de carga 278
Un destino registrado no está operativo 278
Los clientes no pueden conectarse a un equilibrador de carga orientado a Internet 280
El equilibrador de carga no recibe las solicitudes enviadas a un dominio personalizado 280
Las solicitudes HTTPS que se envían al equilibrador de carga devuelven "NET: :ERR_CERT_COMMON_NAME_INVALID" 281
El equilibrador de carga muestra tiempos de procesamiento elevados 281
El equilibrador de carga envía un código de respuesta 000 282
El equilibrador de carga genera un error HTTP 282
HTTP 400: Solicitud errónea 283
HTTP 401: No autorizado 283
HTTP 403: Prohibido 283
HTTP 405: Método no permitido 284
HTTP 408: Request timeout 284
HTTP 413: Carga demasiado grande 284
HTTP 414: URI demasiado largo 284
HTTP 460 284
HTTP 463 284
HTTP 464 285
HTTP 500: Error interno del servidor 285
HTTP 501: No implementado 285
HTTP 502: Bad puerta de enlace 286
HTTP 503: Service unavailable 286
HTTP 504: Gateway timeout 286
HTTP 505: Versión no compatible 287
HTTP 507: almacenamiento insuficiente 287
HTTP 561: No autorizado 287
Hay un destino que genera un error HTTP 287

No hay ningún AWS Certificate Manager certificado disponible para su uso 288
No se admiten encabezados de varias líneas 288
Solucione los problemas de los objetivos en mal estado mediante el mapa de recursos 288
Cuotas 291
Historial de documentos 295
..... cccii

¿Qué es un Equilibrador de carga de aplicación?

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

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

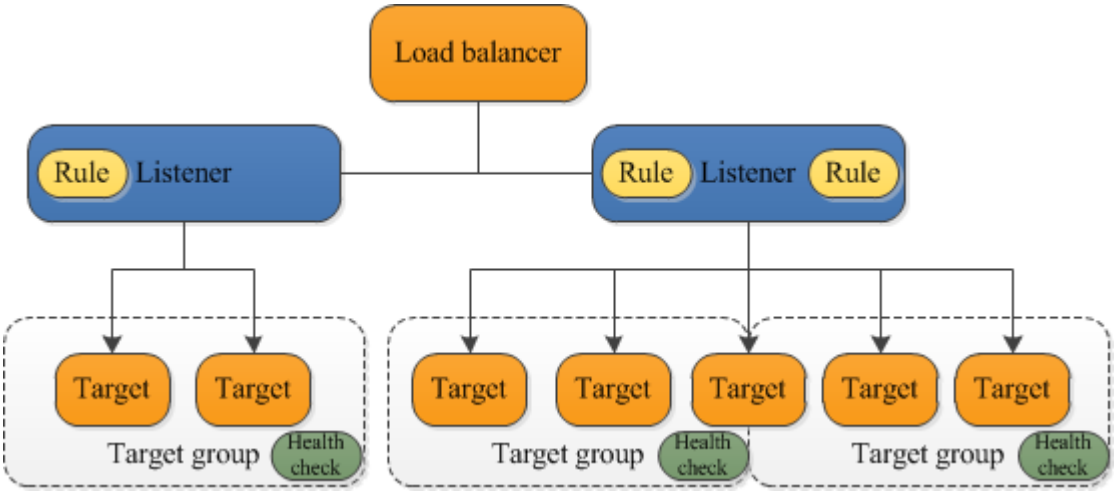
Componentes del Equilibrador de carga de aplicación

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

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

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

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



Para obtener más información, consulte la siguiente documentación sobre :

- Equilibradores de carga
- Oyentes
- Grupos de destino

Información general sobre Equilibrador de carga de aplicación

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

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

de carga a medida que va cambiando el tráfico dirigido a la aplicación con el tiempo. Elastic Load Balancing puede escalarse automáticamente para adaptarse a la mayoría de las cargas de trabajo.

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

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

Ventajas de migrar desde un Equilibrador de carga clásico

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

- Compatibilidad con Condiciones de ruta. Puede configurar reglas para el oyente que reenvíen las solicitudes en función de la dirección URL contenida en la solicitud. Esto permite estructurar la aplicación en servicios de menor tamaño y direccionar las solicitudes al servicio correcto según el contenido de la URL.
- Compatibilidad con Condiciones de host. Puede configurar reglas para el oyente que reenvíen las solicitudes en función del campo de host en el encabezado HTTP. Esto permite direccionar solicitudes a varios dominios a través de un único equilibrador de carga.
- Compatibilidad para direccionamiento basado en campos en la solicitud, como, por ejemplo, Condiciones de los encabezados HTTP y métodos, parámetros de la consulta y direcciones IP de origen.
- Compatibilidad con el direccionamiento de solicitudes a varias aplicaciones en una sola instancia EC2. Puede registrar cada instancia o dirección IP con múltiples grupos de destino utilizando varios puertos.
- Compatibilidad con el redireccionamiento de solicitudes de una URL a otra.
- Compatibilidad con la devolución de una respuesta HTTP personalizada.
- Compatibilidad con el registro de destinos por dirección IP, incluidos los destinos situados fuera de la VPC para el equilibrador de carga.
- Compatibilidad para registrar funciones de Lambda como destinos.
- Compatibilidad para que el equilibrador de carga pueda autenticar a los usuarios de sus aplicaciones a través de sus identidades corporativas o sociales antes de enviar solicitudes.

- Compatibilidad con las aplicaciones en contenedores. Amazon Elastic Container Service (Amazon ECS) permite seleccionar un puerto no utilizado al programar una tarea y registrarla en un grupo de destino mediante este puerto. De este modo, puede hacer un uso eficiente de los clústeres.
- Support para monitorear el estado de cada servicio de forma independiente, ya que los controles de estado se definen a nivel del grupo objetivo y muchas CloudWatch métricas se informan a nivel del grupo objetivo. Si adjunta un grupo de destino a un grupo de escalado automático, podrá escalar cada servicio de forma dinámica en función de la demanda.
- Los registros de acceso contienen información adicional y se almacenan en formato comprimido.
- Mejora del desempeño del equilibrador de carga.

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

Servicios de relacionados

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

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

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

- AWS Global Accelerator: mejora la disponibilidad y el rendimiento de la aplicación. Utilice un acelerador para distribuir el tráfico entre varios equilibradores de carga en una o varias regiones de AWS. Para obtener más información, consulte la Guía para desarrolladores de AWS Global Accelerator.
- Route 53 ofrece una forma rentable y de confianza de direccionar a los visitantes a los sitios web convirtiendo los nombres de dominio (como `www.example.com`) en direcciones IP numéricas (como `192.0.2.1`) que los equipos utilizan para comunicarse entre sí. AWS asigna URL a sus recursos, como equilibradores de carga. No obstante, puede ser conveniente utilizar una URL que los usuarios puedan recordar fácilmente. Por ejemplo, puede asignar el nombre de dominio a un equilibrador de carga. Para obtener más información, consulte Enrutamiento del tráfico a un equilibrador de carga de ELB en la Guía para desarrolladores de Amazon Route 53.
- AWS WAF: Use AWS WAF con su Equilibrador de carga de aplicación para permitir o bloquear las solicitudes en función de las reglas de una lista de control de acceso web (ACL web). Para obtener más información, consulte Equilibradores de carga de aplicaciones y AWS WAF.

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

Precios

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

Introducción a los equilibradores de carga de aplicaciones

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

Tareas

- Antes de empezar
- Paso 1: Configurar un grupo de destino
- Paso 2: Elegir un tipo de equilibrador de carga
- Paso 3: Configurar un equilibrador de carga y un oyente
- Paso 4: Probar un equilibrador de carga
- Paso 5: (Opcional) Eliminar el equilibrador de carga

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

Antes de empezar

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

Paso 1: Configurar un grupo de destino

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

Para configurar su grupo objetivo mediante la consola

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

Paso 2: Elegir un tipo de equilibrador de carga

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

Para crear un Application Load Balancer mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En la barra de navegación, elija una región para el equilibrador de carga. No olvide elegir la misma región que utilizó con las instancias EC2.
3. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
4. Elija Create Load Balancer (Crear equilibrador de carga).
5. Para Equilibrador de carga de aplicación (Balanceador de carga de aplicaciones), elija Create (Crear).

Paso 3: Configurar un equilibrador de carga y un oyente

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

Para configurar el equilibrador de carga y el oyente

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

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

Paso 4: Probar un equilibrador de carga

Después de crearlo, puede comprobar si el tráfico se envía a las instancias EC2.

Para probar el equilibrador de carga

1. Una vez que se le notifique que el equilibrador de carga se ha creado correctamente, elija Close.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el grupo de destino que se acaba de crear.
4. Elija Targets y verifique que las instancias estén listas. Si el estado de una instancia es `initial`, puede deberse a que la instancia sigue en proceso de registro o no ha superado el número mínimo de comprobaciones de estado para que se considere correcta. Cuando el estado de al menos una instancia sea `healthy`, podrá probar el equilibrador de carga.
5. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
6. Seleccione el equilibrador de carga recién creado.
7. Elija Descripción y copie el nombre DNS del balanceador de cargas (por ejemplo, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com). Pegue el nombre DNS en el campo de direcciones de un navegador web que esté conectado a Internet. Si todo funciona normalmente, el navegador mostrará la página predeterminada del servidor.
8. (Opcional) Para definir reglas de oyente adicionales, consulte Agregar una regla.

Paso 5: (Opcional) Eliminar el equilibrador de carga

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

Para eliminar el balanceador de cargas mediante la consola

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

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

Tutorial: Crear un Equilibrador de carga de aplicación con AWS CLI

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

Antes de empezar

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

  ```
  aws elbv2 help
  ```

  Si aparece un mensaje de error en el que se indica que elbv2 no es una opción válida, actualice AWS CLI. Para obtener más información, consulte Installing the AWS Command Line Interface en la Guía del usuario de AWS Command Line Interface .
- Lance las instancias EC2 en una nube privada virtual (VPC). Asegúrese de que los grupos de seguridad de estas instancias permiten obtener acceso al puerto del oyente y al puerto de comprobación de estado. Para obtener más información, consulte Grupos de seguridad de destino.
- Decida si va a crear un equilibrador de carga IPv4 o de doble pila. Utilice IPv4 si desea que los clientes se comuniquen con el equilibrador de carga solo mediante direcciones IPv4. Utilice la pila doble si desea que los clientes se comuniquen con el equilibrador de carga mediante direcciones IPv4 e IPv6. También puede utilizar la pila doble para comunicarse con destinos de backend, como aplicaciones IPv6 o subredes de pila doble, mediante IPv6.
- Asegúrese de instalar un servidor web, como Apache o Internet Information Services (IIS), en cada instancia EC2. Asegúrese de que los grupos de seguridad de estas instancias permitan el acceso HTTP en el puerto 80.

Crear el equilibrador de carga

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

Para crear un equilibrador de carga

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

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

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

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

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

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

2. Utilice el create-target-groupcomando para crear un grupo de destino, especificando la misma VPC que utilizó para las instancias de EC2.

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

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

   El resultado contiene el ARN del grupo con este formato:

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

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

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
```

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

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

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

   El resultado contiene el ARN del oyente con el siguiente formato:

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

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

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

Adición de un oyente HTTPS

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

Para agregar un oyente HTTPS a un equilibrador de carga

1. Cree un certificado SSL para usarlo con el equilibrador de carga a través de uno de estos métodos:
   - Cree o importe el certificado mediante AWS Certificate Manager (ACM). Para obtener más información, consulte Solicitud de un certificado o Importación de certificados en la Guía del usuario de AWS Certificate Manager .
   - Cargue el certificado mediante AWS Identity and Access Management (IAM). Para obtener más información, consulte Working with Server Certificates (Trabajar con certificados de servidores) en la Guía para el usuario de IAM.
2. Utilice el comando create-oyente para crear el oyente con una regla predeterminada que reenvíe las solicitudes al grupo de destino. Cuando cree un oyente HTTPS, deberá especificar

un certificado SSL. Tenga en cuenta que puede especificar una política SSL que no sea la predeterminada a través de la opción `--ssl-policy`.

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

Agregar direccionamiento basado en rutas

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

Para agregar una regla a un oyente usando un patrón de ruta

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

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

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

```
aws elbv2 register-targets --target-group-arn targetgroup-arn  \
--targets Id=i-0abcdef1234567890 Id=i-1234567890abcdef0
```

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

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

Eliminar el equilibrador de carga

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

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

equilibrador de carga de aplicaciones

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

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

Contenido

- Subredes del equilibrador de carga
- Grupos de seguridad del equilibrador de carga
- Estado del equilibrador de carga
- Atributos del equilibrador de carga
- Tipo de dirección IP
- Mapa de recursos de Application Load Balancer
- Conexiones del balanceador de carga
- Equilibrio de carga entre zonas
- Protección contra eliminación
- Modo de mitigación de desincronización
- Conservación del encabezado del host
- Equilibradores de carga de aplicaciones y AWS WAF
- Creación de un Equilibrador de carga de aplicación
- Zonas de disponibilidad del Equilibrador de carga de aplicación
- Grupos de seguridad para el Equilibrador de carga de aplicación
- Tipos de direcciones IP para el Equilibrador de carga de aplicación
- Etiquetas del Equilibrador de carga de aplicación
- Eliminación de un Equilibrador de carga de aplicación
- Cambio de zona

Subredes del equilibrador de carga

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

Consideraciones

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

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

Tipos de subred

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

Subredes de zona de disponibilidad

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

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

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

Subredes de zona local

Puede especificar una o más subredes de zona local. Se aplican las siguientes restricciones:

- No se puede usar AWS WAF con el balanceador de carga.
- No podrá utilizar una función de Lambda como destino.
- No puedes usar sesiones fijas ni aplicaciones adhesivas.

Subredes de Outpost

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

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

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

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

Grupos de seguridad del equilibrador de carga

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

Las reglas de los grupos de seguridad que están asociados con el equilibrador de carga deben permitir el tráfico en ambas direcciones tanto en el oyente como en los puertos de comprobación de estado. Siempre que se agrega un oyente a un equilibrador de carga o se actualiza el puerto de comprobación de estado de un grupo de destino, es preciso revisar las reglas del grupo de seguridad con el fin de asegurarse de que permitan el tráfico en el nuevo puerto en ambas direcciones. Para obtener más información, consulte Reglas recomendadas.

Estado del equilibrador de carga

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

`provisioning`

El equilibrador de carga se está configurando.

`active`

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

`active_impaired`

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

`failed`

El equilibrador de carga no se han podido configurar.

Atributos del equilibrador de carga

A continuación se indican los atributos del equilibrador de carga:

`access_logs.s3.enabled`

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

`access_logs.s3.bucket`

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

`access_logs.s3.prefix`

Prefijo de la ubicación en el bucket de Amazon S3.

`client_keep_alive.seconds`

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

`deletion_protection.enabled`

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

`idle_timeout.timeout_seconds`

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

`ipv6.deny_all_igw_traffic`

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

`routing.http.desync_mitigation_mode`

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

`routing.http.drop_invalid_header_fields.enabled`

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

`routing.http.preserve_host_header.enabled`

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

`routing.http.x_amzn_tls_version_and_cipher_suite.enabled`

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

`routing.http.xff_client_port.enabled`

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

`routing.http.xff_header_processing.mode`

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

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

`routing.http2.enabled`

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

`waf.fail_open.enabled`

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

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

Tipo de dirección IP

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

Los balanceadores de carga de aplicaciones admiten los siguientes tipos de direcciones IP:

`ipv4`

Los clientes deben conectarse al equilibrador de carga mediante direcciones IPv4 (por ejemplo, 192.0.2.1)

`dualstack`

Los clientes pueden conectarse al equilibrador de carga mediante direcciones IPv4 (por ejemplo, 192.0.2.1) y direcciones IPv6 (por ejemplo, 2001:0db8:85a3:0:0:8a2e:0370:7334).

Consideraciones

- El equilibrador de carga se comunica con los destinos en función del tipo de dirección IP del grupo de destino.
- Cuando habilita el modo de doble pila para el equilibrador de carga, Elastic Load Balancing proporciona un registro DNS AAAA para el equilibrador de carga. Los clientes que se

comunican con el equilibrador de carga mediante direcciones IPv4 resuelven el registro DNS A. Los clientes que se comunican con el equilibrador de carga mediante direcciones IPv6 resuelven el registro DNS AAAA.

- El acceso a los equilibradores de carga internos de doble pila a través de la puerta de enlace de Internet está bloqueado para evitar el acceso no deseado a Internet. Sin embargo, esto no impide el acceso a Internet que no sea de IGW (por ejemplo, mediante peering, AWS Direct Connect Transit Gateway o). AWS VPN

`dualstack-without-public-ipv4`

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

Consideraciones

- La autenticación Application Load Balancer solo admite IPv4 cuando se conecta a un proveedor de identidad (IdP) o a un punto de conexión de Amazon Cognito. Sin una dirección IPv4 pública, el balanceador de cargas no puede completar el proceso de autenticación, lo que provoca errores HTTP 500.

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

Mapa de recursos de Application Load Balancer

El mapa de recursos de Application Load Balancer proporciona una visualización interactiva de la arquitectura del balanceador de cargas, incluidos los oyentes, las reglas, los grupos objetivo y los objetivos asociados. El mapa de recursos también destaca las relaciones y las rutas de enrutamiento entre todos los recursos, lo que proporciona una representación visual de la configuración del balanceador de cargas.

Para ver el mapa de recursos del balanceador de carga de aplicaciones mediante la consola

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

Componentes del mapa de recursos

Vistas de mapas

Hay dos vistas disponibles en el mapa de recursos de Application Load Balancer: Overview y Unhealthy Target Map. La descripción general está seleccionada de forma predeterminada y muestra todos los recursos del balanceador de cargas. Al seleccionar la vista del mapa de objetivos en mal estado, solo se mostrarán los objetivos en mal estado y los recursos asociados a ellos.

La vista del mapa de objetivos en mal estado se puede utilizar para solucionar problemas de objetivos que no pasen los controles de estado. Para obtener más información, consulte Solucione los problemas de los objetivos en mal estado mediante el mapa de recursos.

Grupos de recursos

El mapa de recursos de Application Load Balancer contiene cuatro grupos de recursos, uno para cada tipo de recurso. Los grupos de recursos son Listeners, Rules, Target groups y Targets.

Mosaicos de recursos

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

- Al pasar el ratón sobre un mosaico de recursos, se resaltan las relaciones entre este y otros recursos.
- Al seleccionar un mosaico de recursos, se resaltan las relaciones entre este y otros recursos y se muestran detalles adicionales sobre ese recurso.
  - condiciones de la regla: las condiciones de cada regla.
  - resumen de salud del grupo destinatario: número de objetivos registrados para cada estado de salud.
  - estado de salud objetivo El estado de salud actual y la descripción del objetivo.

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

- Cada mosaico de recursos contiene un enlace que, cuando se selecciona, lleva a la página de detalles de ese recurso.

- Listeners - Seleccione el protocolo de oyentes: puerto. Por ejemplo, `HTTP:80`
- Reglas - Seleccione la acción de las reglas. Por ejemplo, `Forward to target group`
- Grupos objetivo - Seleccione el nombre del grupo objetivo. Por ejemplo, `my-target-group`
- Objetivos - Seleccione el ID del objetivo. Por ejemplo, `i-1234567890abcdef0`

Exporte el mapa de recursos

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

Conexiones del balanceador de carga

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

Tiempo de inactividad de conexión

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

Para garantizar que las operaciones prolongadas, como la carga de archivos, tengan tiempo de completarse, envíe al menos 1 byte de datos antes de que transcurra cada período de inactividad y aumente la duración del período de inactividad según sea necesario. También recomendamos que configure el tiempo de inactividad de su aplicación para que sea mayor que el tiempo de inactividad configurado para el equilibrador de carga. De lo contrario, si la aplicación cierra la conexión TCP al equilibrador de carga de forma irregular, este podría enviar una solicitud a la aplicación antes de que reciba el paquete que indica que la conexión está cerrada. Si este es el caso, entonces el equilibrador de carga envía un error HTTP 502 Bad Gateway al cliente.

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

Para actualizar el valor del tiempo de espera de inactividad de la conexión mediante la consola

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

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

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

El tiempo de mantenimiento de la vida del cliente HTTP

La duración de mantenimiento del cliente HTTP es el tiempo máximo durante el que Application Load Balancer mantendrá una conexión HTTP persistente con un cliente. Una vez transcurrido el tiempo de conservación del cliente HTTP configurado, Application Load Balancer acepta una solicitud y devuelve una respuesta que cierra la conexión sin problemas.

El tipo de respuesta que envía el balanceador de cargas depende de la versión HTTP utilizada por la conexión del cliente. Para los clientes conectados mediante HTTP 1.x, el balanceador de cargas envía un encabezado HTTP que contiene el campo. `Connection: close` Para los clientes conectados mediante HTTP/2, el balanceador de cargas envía un marco. `GOAWAY`

De forma predeterminada, los balanceadores de carga de aplicaciones establecen el valor de duración de keepalive del cliente HTTP en 3600 segundos o 1 hora. La duración de mantenimiento del cliente HTTP no se puede desactivar ni establecer por debajo del mínimo de 60 segundos, pero puede aumentarla hasta un máximo de 60 800 segundos, o 7 días. El Application Load Balancer comienza el período de conservación del cliente HTTP cuando se establece inicialmente una conexión HTTP con un cliente. El período de duración continúa cuando no hay tráfico y no se restablece hasta que se establece una nueva conexión.

> **Note**
>
> Al cambiar el tipo de dirección IP de su Application Load Balancer por `dualstack-without-public-ipv4` el balanceador de carga, espera a que se completen todas las conexiones activas. Para reducir el tiempo que se tarda en cambiar el tipo de dirección IP del balanceador de carga de aplicaciones, considere reducir la duración del mantenimiento del cliente HTTP.

El Application Load Balancer asigna al cliente HTTP la duración keepalive una vez durante la conexión inicial. Al actualizar la duración de keepalive del cliente HTTP, esto puede provocar conexiones simultáneas con diferentes valores de duración de keepalive del cliente HTTP. Las conexiones existentes conservarán el valor de duración de keepalive del cliente HTTP aplicado durante su conexión inicial, mientras que cualquier conexión nueva recibirá el valor de duración keepalive del cliente HTTP actualizado.

Para actualizar el valor de duración de keepalive del cliente mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración de tráfico, introduzca un valor para la duración del mantenimiento activo del cliente HTTP. El intervalo válido es de 60 a 604800 segundos.
6. Elija Guardar cambios.

Para actualizar el valor de duración de keepalive del cliente mediante el AWS CLI

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

Equilibrio de carga entre zonas

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

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

Protección contra eliminación

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

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

Para habilitar la protección contra eliminación desde la consola

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

Para deshabilitar la protección contra eliminación desde la consola

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

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

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

Modo de mitigación de desincronización

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

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

Clasificaciones

Las clasificaciones son las siguientes:

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

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

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

Modos

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

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

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

Para actualizar el modo de mitigación de desincronización mediante la consola

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

Para actualizar el modo de mitigación de la desincronización mediante el AWS CLI

Use el comando modify-load-balancer-attributes con el atributo `routing.http.desync_mitigation_mode` establecido en `monitor`, `defensive` o `strictest`.

Conservación del encabezado del host

Cuando habilita el atributo Conservar encabezado de host, el Equilibrador de carga de aplicación conserva el encabezado `Host` de la solicitud HTTP y la envía a los destinos sin ninguna

modificación. Si el Equilibrador de carga de aplicación recibe varios encabezados `Host`, los conserva todos. Las reglas de oyente se aplican solo al primer encabezado `Host` recibido.

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

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

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

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

Puerto del oyente	Ejemplo de solicitud	Encabezado de host en la solicitud	La conservación del encabezado del host está deshabilitada (comportamiento predeterminado)	La conservación del encabezado del host está habilitada
La solicitud se envía en el oyente HTTP/HTTPS predeterminado.	`GET / index.html HTTP/1.1 Host: example.com`	example.com	example.com	example.com
La solicitud se envía en el detector HTTP predeterminado y el encabezado del host tiene	`GET / index.html HTTP/1.1 Host: example.com:80`	example.com:80	example.com	example.com:80

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

Para habilitar la conservación del encabezado del host mediante la consola

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

Para habilitar la conservación del encabezado del host mediante AWS CLI

Use el comando modify-load-balancer-attributes con el atributo `routing.http.preserve_host_header.enabled` establecido en `true`.

Equilibradores de carga de aplicaciones y AWS WAF

Puede usarlo AWS WAF con su Application Load Balancer para permitir o bloquear las solicitudes según las reglas de una lista de control de acceso web (ACL web). Para obtener más información, consulte Trabajar con ACL web en la Guía para desarrolladores de AWS WAF .

De forma predeterminada, si el balanceador de cargas no puede obtener una respuesta AWS WAF, devuelve un error HTTP 500 y no reenvía la solicitud. Si necesitas que el balanceador de cargas reenvíe las solicitudes a los destinos aunque no pueda contactar con ellos AWS WAF, puedes habilitar AWS WAF la integración. Para comprobar si tu balanceador de carga se integra con él AWS WAF, selecciona tu balanceador de carga en la pestaña Servicios integrados AWS Management Console y elige la pestaña correspondiente.

ACL web predefinidas

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

- `AWSManagedRulesAmazonIpReputationList`- El grupo de reglas de la lista de reputación IP de Amazon bloquea las direcciones IP que suelen estar asociadas a bots u otras amenazas. Para obtener más información, consulta el grupo de reglas gestionado por la lista de reputación IP de Amazon en la Guía para AWS WAF desarrolladores.

- `AWSManagedRulesCommonRuleSet`- El grupo de reglas básico del conjunto de reglas (CRS) proporciona protección contra la explotación de una amplia gama de vulnerabilidades, incluidas algunas de las vulnerabilidades de alto riesgo y frecuentes que se describen en publicaciones de OWASP, como OWASP Top 10. Para obtener más información, consulte el grupo de reglas gestionado por el conjunto básico de reglas (CRS) en la Guía para desarrolladores.AWS WAF
- `AWSManagedRulesKnownBadInputsRuleSet`- El grupo de reglas de entradas incorrectas conocidas bloquea los patrones de solicitudes que se sabe que no son válidos y que están asociados con la explotación o el descubrimiento de vulnerabilidades. Para obtener más información, consulte el grupo de reglas gestionadas con entradas incorrectas conocidas en la Guía para AWS WAF desarrolladores.

Para habilitar el AWS WAF uso de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Integraciones, expanda el Firewall de aplicaciones AWS web (WAF) y elija Asociar una ACL web de WAF.
5. En ACL web, elija Crear automáticamente una ACL web predefinida o seleccione una ACL web existente.
6. En Acción de regla, elija Bloquear o Contar.
7. Elija Confirmar.

Para activar la apertura en caso de AWS WAF error, utilice la AWS CLI

Use el comando modify-load-balancer-attributes con el atributo `waf.fail_open.enabled` establecido en `true`.

Creación de un Equilibrador de carga de aplicación

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

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

Para crear un equilibrador de carga mediante el AWS CLI, consulteTutorial: Crear un Equilibrador de carga de aplicación con AWS CLI.

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

Tareas

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

Paso 1: Configurar un grupo de destino

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

Para configurar el grupo objetivo mediante la consola

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

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

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

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

    d. Si el tipo de destino es Instancias o direcciones IP, elija IPv4 o IPv6 como tipo de dirección IP; de lo contrario, pase al siguiente paso.

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

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

f. Para la versión de protocolo, seleccione HTTP1 cuando el protocolo de solicitud sea HTTP/1.1 o HTTP/2; seleccione HTTP2, cuando el protocolo de solicitud sea HTTP/2 o gRPC; y seleccione gRPC, cuando el protocolo de solicitud sea gRPC.

5. En la sección Comprobaciones de estado, mantenga la configuración predeterminada. En Configuración avanzada de la comprobación de estado, elija el puerto de comprobación de estado, el recuento, el tiempo de espera y el intervalo, y especifique los códigos de éxito. Si las comprobaciones de estado superan el recuento de UnhealthyThresholdCount, el equilibrador de carga inhabilita el destino. Cuando las comprobaciones de estado superan el recuento de HealthyThresholdCount, el equilibrador de carga vuelve a poner el destino en servicio. Para obtener más información, consulte Comprobaciones de estado de los grupos de destino.

6. (Opcional) Agregue una o varias etiquetas, como se indica a continuación:

   a. Expanda la sección Etiquetas.

   b. Seleccione Agregar etiqueta.

   c. Escriba la clave y el valor de la etiqueta. Los caracteres permitidos son letras, espacios y números (en UTF-8), además de los siguientes caracteres especiales: + - =. _ : / @. No utilice espacios iniciales ni finales. Los valores distinguen entre mayúsculas y minúsculas.

7. Elija Siguiente.

Paso 2: Registrar destinos

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

1. En la página Registrar destinos, agregue uno o más destinos de la siguiente manera:

   - Si el tipo de destino es Instancias, seleccione una o más instancias, introduzca uno o más puertos y, a continuación, elija Incluir como pendiente debajo.
   - Si el tipo de destino es direcciones IP, haga lo siguiente:

a. Seleccione una VPC de red de la lista o elija Otras direcciones IP privadas.
b. Introduzca la dirección IP manualmente o busque la dirección IP mediante los detalles de la instancia. Puede introducir hasta cinco direcciones IP a la vez.
c. Introduzca los puertos para enrutar el tráfico a las direcciones IP especificadas.
d. Seleccione Incluir como pendiente debajo.

- Si el tipo de destino es Lambda, seleccione una función de Lambda o introduzca el ARN de una función de Lambda y, a continuación, seleccione Incluir como pendiente.

2. Elija Crear grupo de destino.

Paso 3: Configurar un equilibrador de carga y un oyente

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

Para configurar el equilibrador de carga y el agente de escucha mediante la consola

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

a. En Load Balancer name (Nombre del equilibrador de carga), escriba un nombre para el equilibrador de carga. Por ejemplo, **`my-alb`**. El nombre de su Equilibrador de carga de aplicación debe ser único dentro del conjunto de equilibradores de carga de aplicaciones y Equilibradores de carga de red para la región. Los nombres pueden tener un máximo de 32 caracteres y solo pueden contener caracteres alfanuméricos y guiones. No pueden comenzar ni terminar con un guion ni con `internal-`. El nombre de su Equilibrador de carga de aplicación no se puede cambiar una vez creado.
b. Para Scheme (Esquema), elija ya sea expuesto a internet o interno. Un equilibrador de carga expuesto a Internet direcciona las solicitudes de los clientes a través de Internet hasta

los destinos. Un equilibrador de carga interno direcciona las solicitudes hasta los destinos mediante direcciones IP privadas.

c. Para el tipo de dirección IP, elige IPv4, Dualstack o Dualstack sin IPv4 público. Elija IPv4 si sus clientes utilizan direcciones IPv4 para comunicarse con el balanceador de cargas. Elija Dualstack si sus clientes utilizan ambas direcciones, IPv4 e IPv6 para comunicarse con el equilibrador de carga. Elija Dualstack sin IPv4 público si sus clientes utilizan únicamente direcciones IPv6 para comunicarse con el balanceador de cargas.

6. Asignación de redes

a. En VPC, seleccione la VPC que ha utilizado para las instancias de EC2. Si seleccionó Con acceso a Internet en Esquema, solo se pueden seleccionar las VPC con una puerta de enlace de Internet.

b. Para los mapeos, habilite las zonas para su equilibrador de carga al seleccionar las subredes de la siguiente manera:

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

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

Para los equilibradores de carga internos, las direcciones IPv4 e IPv6 se asignan desde el CIDR de subred.

Si ha habilitado el modo Doble pila para el equilibrador de carga, seleccione subredes con bloques de CIDR IPv4 e IPv6 asociados.

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

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

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

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

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

   a. En Certificado SSL/TLS 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 Certificate Chain (Cadena del certificado), copie y pegue el contenido del archivo de cadena del certificado (con codificación PEM), a no ser que utilice un certificado autofirmado y no sea importante que los navegadores acepten implícitamente dicho certificado.

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

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

      Si selecciona Verificar con Trust Store:

      - De forma predeterminada, se rechazan las conexiones con certificados de cliente caducados. Para cambiar este comportamiento, expanda la configuración avanzada de mTLS y, en Vencimiento de los certificados de cliente, seleccione Permitir certificados de cliente caducados.

- En Almacén de confianza, selecciona un almacén de confianza existente o elige Nuevo almacén de confianza.
  - Si ha elegido un nuevo almacén de confianza, proporcione un nombre de almacén de confianza, la ubicación de la autoridad de certificación URI de S3 y, si lo desea, una ubicación en la lista de revocaciones de certificados URI de S3.

10. (Opcional) Puedes integrar otros servicios con tu balanceador de cargas durante la creación, en Optimizar con integraciones de servicios.

    - Puede optar por incluir protecciones de AWS WAFseguridad para su balanceador de carga, con una ACL web existente o creada automáticamente. Tras la creación, las ACL web se pueden gestionar en la AWS WAF consola. Para obtener más información, consulte Asociar o desasociar una ACL web a un AWS recurso en la Guía para desarrolladores.AWS WAF
    - Puede optar por AWS Global Acceleratorcrear un acelerador para usted y asociar su balanceador de cargas al acelerador. El nombre del acelerador puede tener los siguientes caracteres (hasta 64 caracteres): a-z, A-Z, 0-9,. (punto) y - (guión). Una vez creado el acelerador, podrá gestionarlo en la AWS Global Accelerator consola. Para obtener más información, consulta Cómo añadir un acelerador al crear un balanceador de cargas en la AWS Global Accelerator Guía para desarrolladores.

11. Etiquetar y crear

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

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

Paso 4: Probar el equilibrador de carga

Una vez que ha creado el equilibrador de carga, puede verificar que las instancias EC2 pasen la comprobación de estado inicial. A continuación, puede comprobar que el equilibrador de carga envía tráfico a su instancia de EC2. Para eliminar el equilibrador de carga, consulte Eliminación de un Equilibrador de carga de aplicación.

Para probar el equilibrador de carga

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

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

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

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

Zonas de disponibilidad del Equilibrador de carga de aplicación

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

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

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

Para actualizar las zonas de disponibilidad desde la consola

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

Para actualizar las zonas de disponibilidad mediante el AWS CLI

Utilice el comando set-subnets.

Grupos de seguridad para el Equilibrador de carga de aplicación

El grupo de seguridad del Equilibrador de carga de aplicación controla el tráfico al que se le permite llegar y dejar el equilibrador de carga. Debe asegurarse de que el equilibrador de carga pueda comunicarse con los destinos registrados en el puerto del oyente y en el puerto de comprobación de estado. Cada vez que agregue un oyente al equilibrador de carga o actualice la comprobación de estado de un grupo de destino que el equilibrador de carga utilice para direccionar solicitudes, debe asegurarse de que los grupos de seguridad asociados a ese equilibrador de carga permitan el tráfico en el nuevo puerto en ambas direcciones. Si no es así, puede editar las reglas de los grupos de seguridad que estén asociados al equilibrador de carga o bien asociarle otros grupos de seguridad. Puede elegir los puertos y los protocolos que desee permitir. Por ejemplo, puede abrir conexiones del Protocolo de mensajes de control de Internet (ICMP) para que el equilibrador de carga responda a las solicitudes de ping (sin embargo, las solicitudes de ping no se reenvían a ninguna instancia).

Reglas recomendadas

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

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

Outbound		
Destination	Port Range	Comment
grupo de seguridad de instancia	*oyente de instancia*	Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia
grupo de seguridad de instancia	*comprobación de estado*	Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado

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

Inbound		
Source	Port Range	Comment
CIDR DE VPC	*oyente*	Permitir el tráfico entrante del CIDR de VPC en el puerto del oyente del equilibrador de carga

Outbound		
Destination	Port Range	Comment

grupo de seguridad de instancia	*oyente de instancia*	Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia
grupo de seguridad de instancia	*comprobación de estado*	Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado

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

Inbound

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

Outbound

Destination	Port Range	Comment
grupo de seguridad de instancia	*oyente de instancia*	Permitir el tráfico saliente a las instancias en el puerto del oyente de la instancia

grupo de seguridad de instancia	*comprobación de estado*	Permitir el tráfico saliente a las instancias en el puerto de comprobación de estado

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

Para asegurarse de que sus objetivos reciban tráfico exclusivamente del balanceador de cargas, restrinja los grupos de seguridad asociados a sus objetivos para que acepten el tráfico únicamente del balanceador de cargas. Esto se puede lograr configurando el grupo de seguridad del balanceador de cargas como origen en la regla de entrada del grupo de seguridad del objetivo.

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 usuario de Amazon EC2.

Actualizar los grupos de seguridad asociados

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

Para actualizar los grupos de seguridad desde la consola

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

Para actualizar los grupos de seguridad mediante el AWS CLI

Utilice el comando set-security-groups.

Tipos de direcciones IP para el Equilibrador de carga de aplicación

Puede configurar su Equilibrador de carga de aplicación para que los clientes puedan comunicarse con el equilibrador de carga mediante únicamente direcciones IPv4 o direcciones IPv4 e IPv6 (doble pila). El equilibrador de carga se comunica con los destinos en función del tipo de dirección IP del grupo de destino. Para obtener más información, consulte Tipo de dirección IP.

Requisitos de la pila doble

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

Para establecer el tipo de dirección IP en la creación

Configure los ajustes como se describe en ???.

Para actualizar el tipo de dirección IP desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Asignación de redes, elija Editar tipo de dirección IP.
5. Para el tipo de dirección IP, elija IPv4 para admitir únicamente direcciones IPv4, Dualstack para admitir direcciones IPv4 e IPv6, o Dualstack sin IPv4 pública para admitir únicamente direcciones IPv6.
6. Elija Guardar cambios.

Para actualizar el tipo de dirección IP mediante el AWS CLI

Utilice el comando set-ip-address-type.

Etiquetas del Equilibrador de carga de aplicación

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

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

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

Restricciones

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

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

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

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

Utilice los comandos add-tags y remove-tags.

Eliminación de un Equilibrador de carga de aplicación

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

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

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

Para eliminar un equilibrador de carga desde la consola

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

   Ejemplo:

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

Para eliminar un balanceador de cargas mediante el AWS CLI

Utilice el comando delete-load-balancer.

Cambio de zona

El cambio de zona es una capacidad del Controlador de recuperación de aplicaciones de Amazon Route 53 (Route 53 ARC). Con el cambio de zona, puede alejar un recurso del equilibrador de carga de una zona de disponibilidad afectada con una sola acción. De esta forma, podrá seguir operando desde otras zonas de disponibilidad en buen estado en una Región de AWS.

Al comenzar un cambio de zona, el equilibrador de carga deja de enviar el tráfico del recurso a la zona de disponibilidad afectada. Route 53 ARC crea el cambio de zona de inmediato. Sin embargo, completar las conexiones existentes y en curso en la zona de disponibilidad afectada puede tardar un tiempo, por lo general unos minutos. Para obtener más información, consulte Cómo funciona un cambio de zona: comprobaciones de estado y direcciones IP de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon Route 53.

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

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

- El equilibrio de carga entre zonas no se admite con cambios de zona. Debe desactivar el equilibrio de carga entre zonas para utilizar esta capacidad.
- El cambio de zona no se admite cuando se utiliza un equilibrador de carga de aplicación como punto de conexión del acelerador en AWS Global Accelerator.
- Puede comenzar un cambio de zona para un equilibrador de carga específico solo para una zona de disponibilidad única. No puede comenzar un cambio de zona para varias zonas de disponibilidad.
- AWS elimina de forma proactiva las direcciones IP del equilibrador de carga de zona del DNS cuando varios problemas de infraestructura afectan a los servicios. Compruebe siempre la capacidad actual de la zona de disponibilidad antes de comenzar un cambio de zona. Si sus equilibradores de carga tienen desactivado el equilibrio de carga entre zonas y utiliza un cambio de zona para eliminar la dirección IP del equilibrador de carga de zona, la zona de disponibilidad afectada por el cambio de zona también pierde la capacidad de destino.

- Cuando un equilibrador de carga de aplicación sea el destino de un equilibrador de carga de red, comience siempre el cambio de zona desde el equilibrador de carga de red. Si comienza un cambio de zona desde el equilibrador de carga de aplicación, el equilibrador de carga de red no reconoce el cambio y continúa enviando tráfico al equilibrador de carga de aplicación.

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

Comenzar un cambio de zona

En los pasos de este procedimiento se explica cómo comenzar un cambio de zona mediante la consola de Amazon EC2. Para conocer los pasos a fin de comenzar un cambio de zona mediante la consola de Route 53 ARC, consulte Cómo comenzar un cambio de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon Route 53.

Para comenzar un cambio de zona mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga.
4. En la pestaña de Integraciones, en Controlador de recuperación de aplicaciones de Route 53, elija Comenzar cambio de zona.
5. Seleccione la zona de disponibilidad de la que desea transferir el tráfico.
6. Elija o ingrese un vencimiento para el cambio de zona. Inicialmente, un cambio de zona se puede configurar desde 1 minuto hasta tres días (72 horas).

   Todos los cambios de zona son temporales. Debe establecer un vencimiento, pero puede actualizar los cambios activos más adelante para establecer un vencimiento nuevo.
7. Ingrese un comentario. Si lo desea, puede actualizar el cambio de zona más adelante para editar el comentario.
8. Seleccione la casilla de verificación para confirmar que comenzar un cambio de zona reducirá la capacidad de su aplicación al cambiar el tráfico de la zona de disponibilidad.
9. Elija Start (Inicio).

Para comenzar un cambio de zona mediante la AWS CLI

Para trabajar con el cambio de zona de forma programática, consulta la Guía de referencia de la API del cambio de zona.

Actualizar un cambio de zona

En los pasos de este procedimiento se explica cómo actualizar un cambio de zona mediante la consola de Amazon EC2. Para conocer los pasos a fin de actualizar un cambio de zona mediante la consola del Controlador de recuperación de aplicaciones de Amazon Route 53, consulte Cómo actualizar un cambio de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon Route 53.

Para actualizar un cambio de zona mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione un nombre de equilibrador de carga que tenga un cambio de zona activo.
4. En la pestaña de Integraciones, en Controlador de recuperación de aplicaciones de Route 53, elija Actualizar cambio de zona.

   Esto abre la consola de Route 53 ARC para continuar con la actualización.
5. En Establecer vencimiento del cambio de zona, si lo desea, seleccione o ingrese un vencimiento.
6. En Comentario, si lo desea, edite el comentario existente o ingrese uno nuevo.
7. Elija Actualizar.

Para actualizar un cambio de zona mediante la AWS CLI

Para trabajar con el cambio de zona de forma programática, consulta la Guía de referencia de la API del cambio de zona.

Cancelar un cambio de zona

En los pasos de este procedimiento se explica cómo cancelar un cambio de zona mediante la consola de Amazon EC2. Para conocer los pasos a fin de cancelar un cambio de zona mediante la consola del Controlador de recuperación de aplicaciones de Amazon Route 53, consulte Cómo cancelar un cambio de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon Route 53.

Para cancelar un cambio de zona mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione un nombre de equilibrador de carga que tenga un cambio de zona activo.
4. En la pestaña de Integraciones, en Controlador de recuperación de aplicaciones de Route 53, elija Cancelar cambio de zona.

   Esto abre la consola de Route 53 ARC para continuar con la cancelación.
5. Elija Cancelar cambio de zona.
6. En el cuadro de diálogo de confirmación, elija Confirmar.

Para cancelar un cambio de zona mediante la AWS CLI

Para trabajar con el cambio de zona de forma programática, consulta la Guía de referencia de la API del cambio de zona.

Oyentes para Equilibrador de carga de aplicación

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

Contenido

- Configuración del oyente
- Reglas del oyente
- Tipos de acción de regla
- Tipos de condición de las reglas
- Crear un oyente HTTP para su equilibrador de carga de aplicaciones
- Crear un oyente HTTPS para el equilibrador de carga de aplicaciones
- Reglas del oyente del equilibrador de carga de aplicaciones
- Actualizar un oyente HTTPS para el equilibrador de carga de aplicaciones
- Autenticación mutua con TLS en Application Load Balancer
- Autenticación de usuarios mediante un Equilibrador de carga de aplicación
- Encabezados HTTP y balanceadores de tipo equilibrador de carga de aplicaciones
- Etiquetas para sus oyentes y reglas
- Eliminar un oyente de Equilibrador de carga de aplicación

Configuración del oyente

Los oyentes son compatibles con los siguientes protocolos y puertos:

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

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

Para obtener más información, consulte Crear un oyente HTTPS para el equilibrador de carga de aplicaciones.

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

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

Los equilibradores de carga de apliación proporcionan soporte nativo para HTTP/2 con oyentes HTTPS. Puede enviar hasta 128 solicitudes a la vez con una conexión HTTP/2. Se puede usar la versión del protocolo para enviar la solicitud a los destinos mediante HTTP/2. Para obtener más información, consulte Versión del protocolo. Como HTTP/2 usa las conexiones frontend de una forma más eficaz, es posible que observe que se establecen menos conexiones entre los clientes y el equilibrador de carga. No puede utilizar la característica server-push de HTTP/2.

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

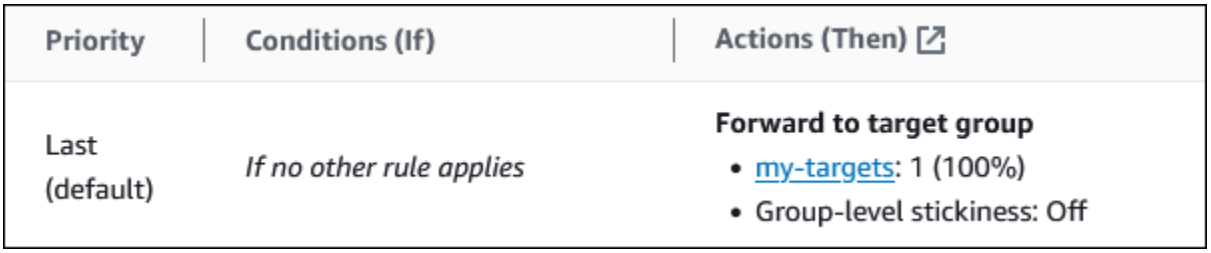
Reglas del oyente

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

Reglas predeterminadas

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

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



Prioridad de las reglas

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

Acciones de las reglas

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

Condiciones de las reglas

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

Tipos de acción de regla

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

`authenticate-cognito`

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

`authenticate-oidc`

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

`fixed-response`

Devuelve una respuesta HTTP personalizada. Para obtener más información, consulte Acciones de respuesta fija.

`forward`

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

`redirect`

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

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

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

Acciones de respuesta fija

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

Cuando se ejecuta una acción `fixed-response`, la acción y la URL del destino se graban en los registros de acceso. Para obtener más información, consulte Entradas de los registros de acceso. El número de acciones `fixed-response` correctas se registra en la métrica `HTTP_Fixed_Response_Count`. Para obtener más información, consulte Métricas del Equilibrador de carga de aplicación.

Example Ejemplo de acción de respuesta fija para el AWS CLI

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

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

Acciones de reenvío

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

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

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

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

Example Ejemplo de acción de reenvío con un grupo de destino

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

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

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

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

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

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

Example Ejemplo de acción de reenvío con la persistencia activada

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

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

```
[
  {
      "Type": "forward",
      "ForwardConfig": {
          "TargetGroups": [
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/blue-targets/73e2d6bc24d8a067",
                  "Weight": 10
              },
              {
                  "TargetGroupArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:targetgroup/green-targets/09966783158cda59",
                  "Weight": 20
              }
          ],
          "TargetGroupStickinessConfig": {
              "Enabled": true,
              "DurationSeconds": 1000
          }
      }
  }
]
```

Acciones de redirección

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

Un URI está formado por los siguientes componentes:

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

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

protocol

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

hostname

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

port

Puerto (entre 1 y 65535).

ruta

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

consulta

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

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

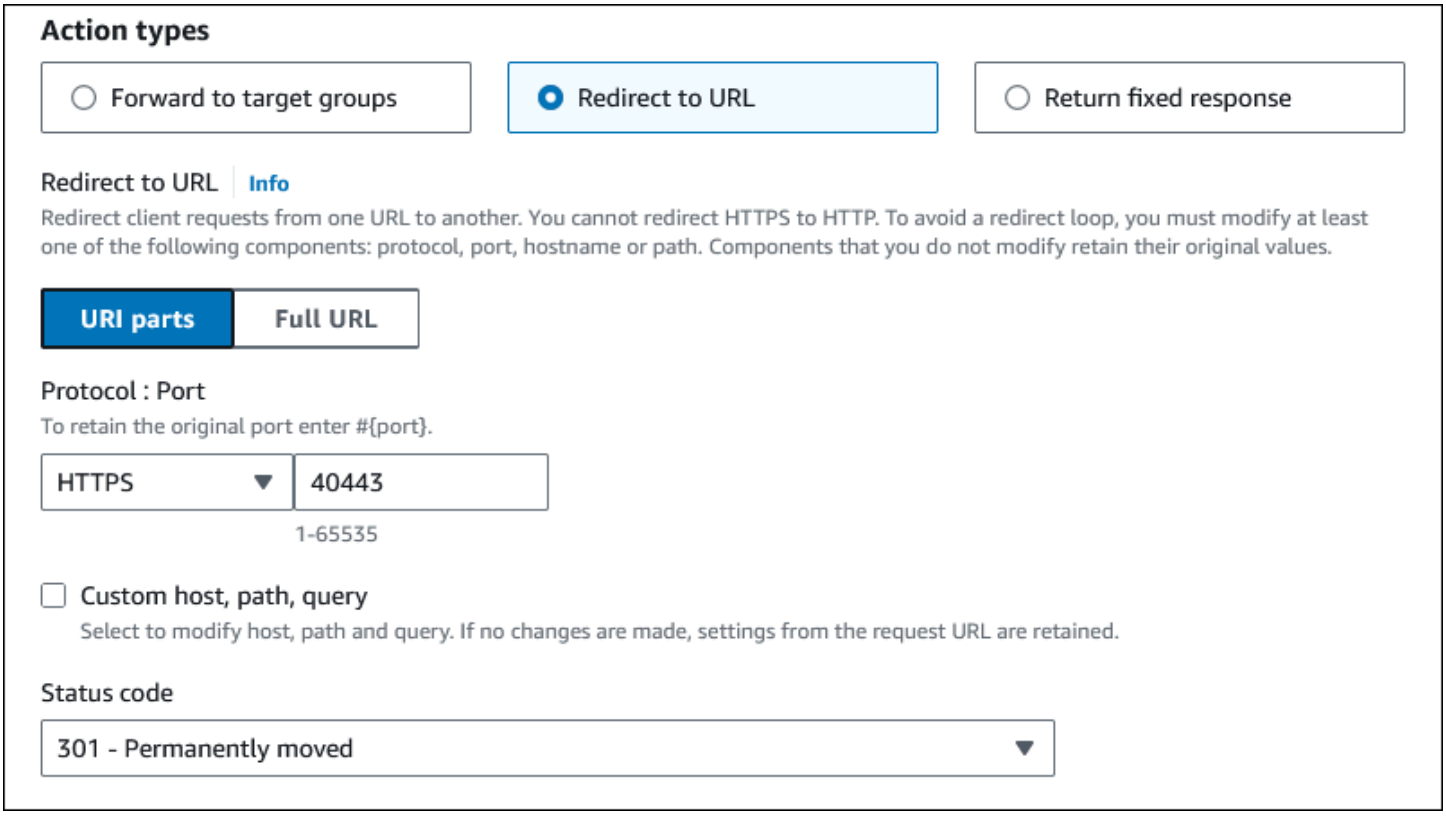
- `#{protocol}` - Mantiene el protocolo. Se usa en los componentes de protocolo y consulta.

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

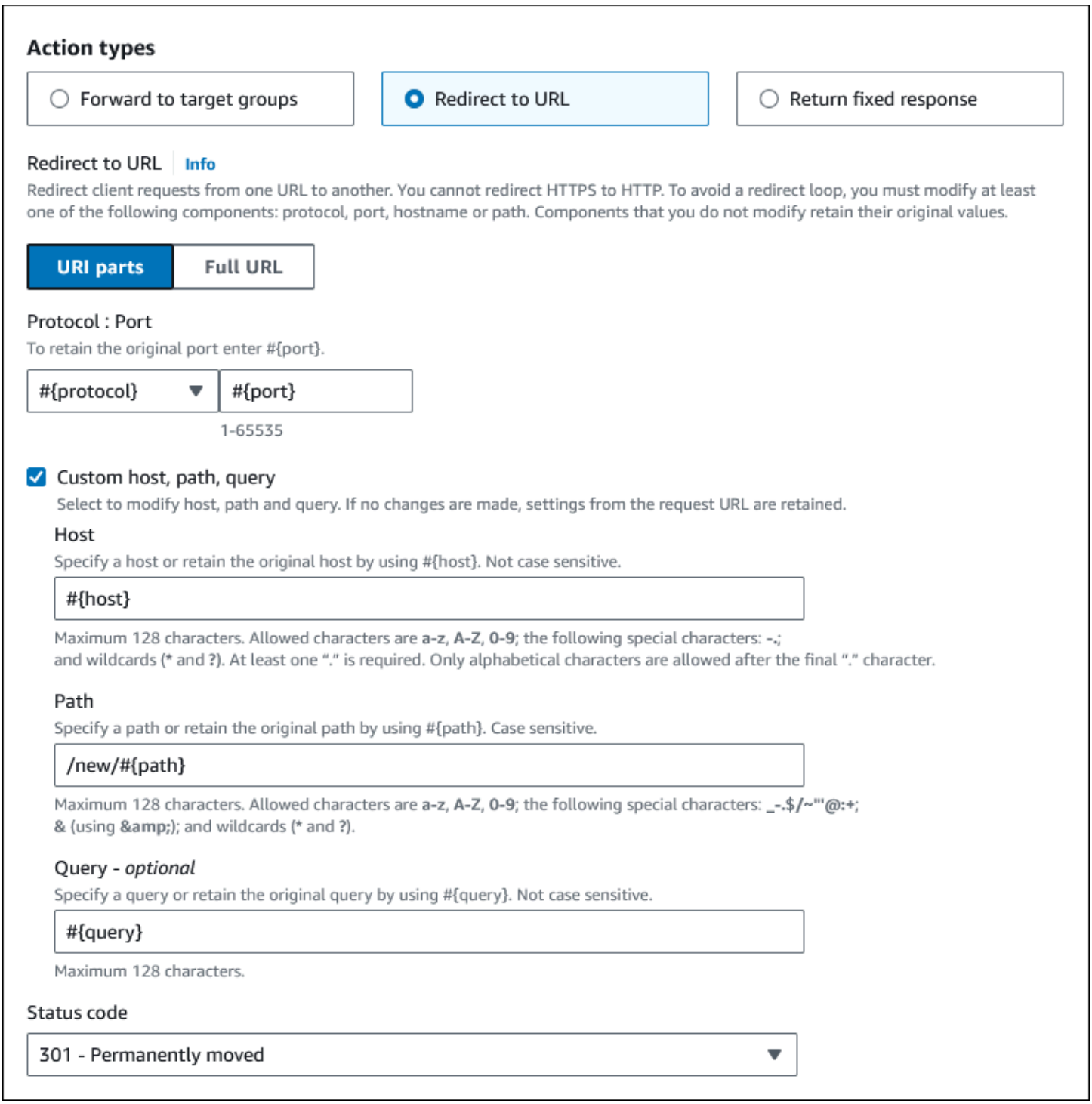
Cuando se ejecuta una acción `redirect`, esta acción se graba en los registros de acceso. Para obtener más información, consulte Entradas de los registros de acceso. El número de acciones `redirect` correctas se registra en la métrica `HTTP_Redirect_Count`. Para obtener más información, consulte Métricas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

Example Ejemplo de acciones de redirección mediante la consola

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



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



Example Ejemplo de acción de redireccionamiento para AWS CLI

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

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

Tipos de condición de las reglas

Se admiten los siguientes tipos de condición para una regla:

`host-header`

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

`http-header`

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

`http-request-method`

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

`path-pattern`

Ruta en función de patrones de ruta en las URL de la solicitud. Para obtener más información, consulte Condiciones de ruta.

`query-string`

Ruta en función de pares clave/valor o en valores en las cadenas de consulta. Para obtener más información, consulte Condiciones de cadena de consulta.

`source-ip`

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

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

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

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

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

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

Para ver demostraciones, consulte Direccionamiento de solicitudes avanzado.

Condiciones de los encabezados HTTP

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

Example Ejemplo de condición de encabezado HTTP para AWS CLI

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

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

Condiciones de método de solicitud HTTP

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

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

Example Ejemplo de condición de método HTTP para AWS CLI

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

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

Condiciones de host

Puede utilizar las condiciones de host para definir reglas que direccionen solicitudes en función del nombre del host en el encabezado del host (lo que también se conoce como direccionamiento

basado en host). Esto permite admitir varios subdominios y diferentes dominios de nivel superior a través de un único equilibrador de carga.

Los nombre de host no distinguen entre mayúsculas y minúsculas, su longitud máxima es de 128 caracteres y pueden contener cualquiera de los siguientes caracteres:

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

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

Ejemplos de nombres de host

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

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

Example Ejemplo de condición de encabezado de host para AWS CLI

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

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

Condiciones de ruta

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

El patrón de ruta se aplica únicamente a la ruta de la dirección URL, no a sus parámetros de consulta. Se aplica solo a los caracteres ASCII visibles; se excluyen los caracteres de control (0x00 a 0x1f y 0x7f).

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

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

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

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

Ejemplos de patrones de ruta HTTP

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

Ejemplos de patrones de ruta gRPC

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

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

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

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

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

Condiciones de cadena de consulta

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

Example Ejemplo de condición de cadena de consulta para AWS CLI

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

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

```
            ]
        }
    }
]
```

Condiciones de dirección IP de origen

Puede utilizar las condiciones de dirección IP de origen para configurar reglas que direccionen solicitudes en función de la dirección IP de origen de la solicitud. La dirección IP se debe especificar en formato CIDR. Puede utilizar tanto direcciones IPv4 como IPv6. No se admiten caracteres comodín. No puede especificar el CIDR `255.255.255.255/32` para la condición de la regla IP de origen.

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

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

Example Ejemplo de condición de IP de origen para AWS CLI

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

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

Crear un oyente HTTP para su equilibrador de carga de aplicaciones

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

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

Requisitos previos

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

Agregar un oyente HTTP

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

Para agregar un oyente HTTPS utilizando la consola

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

    - Reenviar a los grupos de destino: seleccione uno o más grupos de destino a los que reenviar el tráfico. Para añadir grupos de destino, seleccione Añadir grupo de destino. Si utiliza más de un grupo de destino, seleccione una ponderación para cada uno y revise el porcentaje asociado. Debe habilitar la persistencia a nivel de grupo en una regla, si se activó la persistencia en uno o más de los grupos de destino.
    - Redirigir a la URL: especifique la URL a la que se redirigirán las solicitudes de los clientes. Esto se puede hacer al introducir cada parte por separado en la pestaña partes de la URI o al ingrsear la dirección completa en la pestaña URL completa. Puede configurar las acciones

de redirección como temporales (HTTP 302) o permanentes (HTTP 301), en función de sus necesidades para Código de estado.

- Devolver una respuesta fija: especifique el código de respuesta que se devolverá a las solicitudes de los clientes rechazadas. Además, puede especificar el Tipo de contenido y el Cuerpo de la respuesta, pero no son obligatorios.

7. Elija Añadir.

Para añadir un agente de escucha HTTP mediante AWS CLI

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

Crear un oyente HTTPS para el equilibrador de carga de aplicaciones

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

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

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

Los Equilibradores de carga de aplicación no admiten claves ED25519.

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

Contenido

- Certificados de SSL

- Certificado predeterminado
- Lista de certificados
- Renovación de certificados
- Políticas de seguridad
  - Políticas de seguridad de TLS 1.3
  - Políticas de seguridad FIPS
  - Para las políticas admitidas
  - Políticas de seguridad de TLS 1.0 a 1.2
  - Protocolos y cifrados TLS
- Agregar un oyente HTTPS

Certificados de SSL

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

Al crear un certificado para utilizarlo con el equilibrador de carga, debe especificar un nombre de dominio. El nombre de dominio del certificado debe coincidir con el registro del nombre de dominio personalizado para poder verificar la conexión TLS. Si no coinciden, no se cifrará el tráfico.

Debe especificar un nombre de dominio completo (FQDN) para el certificado, por ejemplo, `www.example.com`, o bien un nombre de dominio de ápex, por ejemplo, `example.com`. También puede utilizar un asterisco (*) como comodín para proteger varios nombres de sitios del mismo dominio. Cuando se solicita un certificado comodín, el asterisco (*) debe encontrarse en la posición situada más a la izquierda del nombre de dominio, y solo puede proteger un nivel de subdominio. Por ejemplo, `*.example.com` protege `corp.example.com` y `images.example.com`, pero no puede proteger `test.login.example.com`. Además, tenga en cuenta que `*.example.com` solo protege los subdominios de `example.com`; no protege el dominio desnudo o ápex (`example.com`). El nombre del caracter comodín aparecerá en el campo Sujeto y en la extensión Nombre alternativo del sujeto del certificado. Para obtener más información sobre certificados públicos, consulte Solicitud de un certificado público en la Guía del usuario de AWS Certificate Manager .

Le recomendamos que utilice AWS Certificate Manager (ACM) para crear los certificados del equilibrador de carga. ACM es compatible con los certificados RSA con longitudes de clave de 2048,

3072 y 4096 bits, y con todos los certificados ECDSA. ACM se integra con Elastic Load Balancing, lo que le permite implementar el certificado en el equilibrador de carga. Para obtener más información, consulte la Guía del usuario de AWS Certificate Manager.

Como alternativa, puede utilizar las herramientas SSL/TLS para crear una solicitud de firma de certificado (CSR) y, a continuación, conseguir que una CA firme la CSR para generar un certificado y, a continuación, importar el certificado a ACM o cargarlo en (IAM). AWS Identity and Access Management Para obtener más información sobre la importación de certificados en ACM, consulte Importar certificados en la Guía del usuario de AWS Certificate Manager . Para obtener más información sobre la carga de certificados en IAM, consulte Uso de certificados de servidor en la Guía del usuario de IAM.

Certificado predeterminado

Al crear un oyente HTTPS, debe especificar exactamente un certificado. Este certificado se conoce como certificado predeterminado. Puede sustituir el certificado predeterminado después de crear el oyente HTTPS. Para obtener más información, consulte Reemplazar el certificado predeterminado.

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

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

Lista de certificados

Después de crear un oyente HTTPS, tiene un certificado predeterminado y una lista de certificados vacía. Opcionalmente puede añadir certificados a la lista de certificados para el oyente. El uso de una lista de certificados permite al equilibrador de carga admitir varios dominios en el mismo puerto y proporcionar un certificado diferente para cada dominio. Para obtener más información, consulte Añadir certificados a la lista de certificados.

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

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

Las entradas del registro de acceso del equilibrador de carga indican el nombre de host especificado por el cliente y el certificado presentado al cliente. Para obtener más información, consulte Entradas de los registros de acceso.

Renovación de certificados

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

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

- Los certificados proporcionados por el balanceador de cargas AWS Certificate Manager e implementados en él se pueden renovar automáticamente. ACM intenta renovar los certificados antes de que venzan. Para obtener más información, consulte Renovación administrada en la Guía del usuario de AWS Certificate Manager .
- Si el certificado se importó en ACM, deberá monitorear la fecha de vencimiento del certificado y renovarlo antes de que venza. Para obtener más información, consulte Importación de certificados en la Guía del usuario de AWS Certificate Manager .
- Si importa un certificado en IAM, debe crear un nuevo certificado, importar el nuevo certificado en ACM o IAM, añadir el nuevo certificado al equilibrador de carga y eliminar el certificado caducado del equilibrador de carga.

Políticas de seguridad

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

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

Consideraciones:

- Los Equilibradores de carga de aplicación solo admiten la renegociación de SSL para las conexiones de destino.
- Los equilibradores de carga de aplicaciones no admiten políticas de seguridad personalizadas.
- La `ELBSecurityPolicy-TLS13-1-2-2021-06` política es la política de seguridad predeterminada para los oyentes HTTPS creados con. AWS Management Console
- La `ELBSecurityPolicy-2016-08` política es la política de seguridad predeterminada para los oyentes HTTPS creados con. AWS CLI
- Al crear un agente de escucha HTTPS, es necesario seleccionar una política de seguridad.
  - Recomendamos la política `ELBSecurityPolicy-TLS13-1-2-2021-06` de seguridad, que incluye TLS 1.3 y es compatible con versiones anteriores de TLS 1.2.
- Puede elegir la política de seguridad que se utilice para las conexiones frontales, pero no para las conexiones finales.
  - En el caso de las conexiones de backend, si su oyente de HTTPS utiliza una política de seguridad de TLS 1.3, se utilizará la política de seguridad `ELBSecurityPolicy-TLS13-1-0-2021-06`. De lo contrario, la política de seguridad `ELBSecurityPolicy-2016-08` se utiliza con las conexiones de backend.
- Para cumplir con las normas de seguridad y conformidad que obligan a deshabilitar determinadas versiones del protocolo TLS, o para dar soporte a los clientes antiguos que requieren cifrados obsoletos, puede utilizar una de las políticas de seguridad. `ELBSecurityPolicy-TLS-` Para ver la versión del protocolo TLS para las solicitudes a su Application Load Balancer, habilite el registro de acceso para su balanceador de carga y examine las entradas del registro de acceso correspondientes. Para obtener más información, consulte Registros de acceso de su Application Load Balancer.

- Puedes restringir las políticas de seguridad que están disponibles para los usuarios en todas tus políticas de IAM Cuentas de AWS y de control de servicios (SCP), respectivamente, y AWS Organizations mediante las claves de condición de Elastic Load Balancing. Para obtener más información, consulte las políticas de control de servicios (SCP) en la Guía del usuario AWS Organizations

Políticas de seguridad de TLS 1.3

Elastic Load Balancing proporciona las siguientes políticas de seguridad de TLS 1.3 para los balanceadores de carga de aplicaciones:

- `ELBSecurityPolicy-TLS13-1-2-2021-06`(Recomendado)
- `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06`
- `ELBSecurityPolicy-TLS13-1-1-2021-06`
- `ELBSecurityPolicy-TLS13-1-0-2021-06`
- `ELBSecurityPolicy-TLS13-1-3-2021-06`

Políticas de seguridad FIPS

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

El Estándar Federal de Procesamiento de la Información (FIPS) es un estándar gubernamental de EE. UU. y Canadá que especifica los requisitos de seguridad de los módulos criptográficos que

protegen la información confidencial. Para obtener más información, consulte la Norma Federal de Procesamiento de Información (FIPS) 140 en la página sobre el cumplimiento de las normas de seguridad en la AWS nube.

Todas las políticas FIPS aprovechan el módulo criptográfico AWS-LC validado por FIPS. Para obtener más información, consulte la página del módulo criptográfico AWS-LC en el sitio del Programa de validación de módulos criptográficos del NIST.

Elastic Load Balancing proporciona las siguientes políticas de seguridad FIPS para los balanceadores de carga de aplicaciones:

- `ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`(Recomendado)
- `ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04`
- `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04`

Para las políticas admitidas

Elastic Load Balancing proporciona las siguientes políticas de seguridad compatibles con FS (Forward Secrecy) para los balanceadores de carga de aplicaciones:

- `ELBSecurityPolicy-FS-1-2-Res-2020-10`
- `ELBSecurityPolicy-FS-1-2-Res-2019-08`
- `ELBSecurityPolicy-FS-1-2-2019-08`
- `ELBSecurityPolicy-FS-1-1-2019-08`
- `ELBSecurityPolicy-FS-2018-06`

Políticas de seguridad de TLS 1.0 a 1.2

Elastic Load Balancing proporciona las siguientes políticas de seguridad de TLS 1.0 a 1.2 para los balanceadores de carga de aplicaciones:

- `ELBSecurityPolicy-TLS-1-2-Ext-2018-06`
- `ELBSecurityPolicy-TLS-1-2-2017-01`
- `ELBSecurityPolicy-TLS-1-1-2017-01`
- `ELBSecurityPolicy-2016-08`
- `ELBSecurityPolicy-TLS-1-0-2015-04`
- `ELBSecurityPolicy-2015-05`(idéntico a) **`ELBSecurityPolicy-2016-08`**

Protocolos y cifrados TLS

TLS 1.3

En la siguiente tabla se describen los protocolos y cifrados TLS compatibles con las políticas de seguridad de TLS 1.3 disponibles.

Nota: Se ha eliminado el `ELBSecurityPolicy-` prefijo de los nombres de las políticas de la fila de políticas de seguridad.

Ejemplo: La política de seguridad `ELBSecurityPolicy-TLS13-1-2-2021-06` se muestra como`TLS13-1-2-2021-06`.

Políticas de seguridad	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protocolos TLS							
Protocolo -TLSv1							✓
Protocolo -TLSv1.1						✓	✓
Protocolo -TLSv1.2	✓		✓	✓	✓	✓	✓

Políticas de seguridad	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protocolo: TLSv1.3	✓	✓	✓	✓	✓	✓	✓
Cifrados TLS							
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓

Políticas de seguridad	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-ECDSA-AES128-SHA256	✓			✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓			✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓
ECDHE-RSA-AES128-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓		✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓		✓	✓	✓	✓	✓

Políticas de seguridad	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE-ECDSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓			✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓
AES128-GCM-SHA256				✓	✓	✓	✓
AES128-SHA256				✓	✓	✓	✓
AES128-SHA				✓		✓	✓

Políticas de seguridad	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
AES256-GCM-SHA384				✓	✓	✓	✓
AES256-SHA256				✓	✓	✓	✓
AES256-SHA				✓		✓	✓

Para crear un agente de escucha HTTPS que utilice una política TLS 1.3 mediante la CLI

Use el comando create-listener con cualquier política de seguridad de TLS 1.3.

En el ejemplo se usa la política de seguridad. `ELBSecurityPolicy-TLS13-1-2-2021-06`

```
aws elbv2 create-listener --name my-listener \
--protocol HTTPS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Para modificar un agente de escucha HTTPS para que utilice una política TLS 1.3 mediante la CLI

Use el comando modify-listener con cualquier política de seguridad de TLS 1.3.

En el ejemplo se usa la política de seguridad. `ELBSecurityPolicy-TLS13-1-2-2021-06`

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Para ver las políticas de seguridad utilizadas por un oyente mediante la CLI

Utilice el comando describe-listeners con el de su oyente. `arn`

```
aws elbv2 describe-listeners \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para ver la configuración de una política de seguridad de TLS 1.3 mediante la CLI

Use el comando describe-ssl-policies con cualquier política de seguridad de TLS 1.3.

En el ejemplo se usa la política de seguridad. `ELBSecurityPolicy-TLS13-1-2-2021-06`

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-2021-06
```

FIPS

> **Important**
>
> Las políticas `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` y `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` se proporcionan únicamente para garantizar la compatibilidad con versiones anteriores. Si bien utilizan la criptografía FIPS mediante el módulo FIPS140, es posible que no se ajusten a las directrices más recientes del NIST para la configuración de TLS.

En la siguiente tabla se describen los protocolos y cifrados TLS compatibles con las políticas de seguridad FIPS disponibles.

Nota: Se ha eliminado el `ELBSecurityPolicy-` prefijo de los nombres de las políticas de la fila de políticas de seguridad.

Ejemplo: La política de seguridad `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` se muestra como`TLS13-1-2-FIPS-2023-04`.

Políticas de seguridad	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
Protocolos TLS								
Protocolo -TLSv1								✓
Protocolo - TLSv1.1							✓	✓
Protocolo - TLSv1.2		✓	✓	✓	✓	✓	✓	✓
Protocolo : TLSv1.3	✓	✓	✓	✓	✓	✓	✓	✓
Cifrados TLS								
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128		✓	✓	✓	✓	✓	✓	✓

Políticas de seguridad	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
-GCM-SHA256								
ECDHE-RSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256			✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA				✓		✓	✓	✓

Políticas de seguridad	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES128-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384			✓	✓	✓	✓	✓	✓

Políticas de seguridad	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-RSA-AES256-SHA384			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓	✓
ECDHE-ECDSA-AES256-SHA				✓		✓	✓	✓
AES128-GCM-SHA256					✓	✓	✓	✓
AES128-SHA256					✓	✓	✓	✓
AES128-SHA						✓	✓	✓

Políticas de seguridad	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
AES256-GCM-SHA384					✓	✓	✓	✓
AES256-SHA256					✓	✓	✓	✓
AES256-SHA						✓	✓	✓

Para crear un agente de escucha HTTPS que utilice una política FIPS mediante la CLI

Utilice el comando create-listener con cualquier política de seguridad de FIPS.

En el ejemplo se usa la política de seguridad. `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`

```
aws elbv2 create-listener --name my-listener \
--protocol HTTPS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Para modificar un agente de escucha HTTPS para que utilice una política FIPS mediante la CLI

Utilice el comando modify-listener con cualquier política de seguridad de FIPS.

En el ejemplo se utiliza la política de seguridad. `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`

```
aws elbv2 modify-listener \
```

```
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Para ver las políticas de seguridad utilizadas por un oyente mediante la CLI

Utilice el comando describe-listeners con el de su oyente. `arn`

```
aws elbv2 describe-listeners \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para ver la configuración de una política de seguridad FIPS mediante la CLI

Utilice el comando describe-ssl-policies con cualquier política de seguridad de FIPS.

En el ejemplo se utiliza la política de seguridad. `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04`

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

FS

En la siguiente tabla se describen los protocolos y cifrados TLS compatibles con las políticas de seguridad compatibles con FS disponibles.

Nota: Se ha eliminado el `ELBSecurityPolicy-` prefijo de los nombres de las políticas de la fila de políticas de seguridad.

Ejemplo: La política de seguridad `ELBSecurityPolicy-FS-2018-06` se muestra como`FS-2018-06`.

Políticas de seguridad	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocolos TLS						
Protocolo-TLSv1	✓					✓
Protocolo-TLSv1.1	✓				✓	✓
Protocolo-TLSv1.2	✓	✓	✓	✓	✓	✓
Cifrados TLS						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓		✓	✓	✓	✓

Políticas de seguridad	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-RSA-AES128-SHA256	✓		✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA	✓			✓	✓	✓
ECDHE-RSA-AES128-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓

Políticas de seguridad	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-ECDSA-AES256-SHA384	✓		✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓		✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓			✓	✓	✓
AES128-GCM-SHA256	✓					
AES128-SHA256	✓					
AES128-SHA	✓					

Políticas de seguridad	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
AES256-GCM-SHA384	✓					
AES256-SHA256	✓					
AES256-SHA	✓					

Para crear un agente de escucha HTTPS que utilice una política compatible con FS mediante la CLI

Utilice el comando create-listener con cualquier política de seguridad compatible con FS.

En el ejemplo se usa la política de seguridad`ELBSecurityPolicy-FS-2018-06`.

```
aws elbv2 create-listener --name my-listener \
--protocol HTTPS --port 443 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Para modificar un agente de escucha HTTPS para que utilice una política compatible con FS mediante la CLI

Utilice el comando modify-listener con cualquier política de seguridad compatible con FS.

En el ejemplo se utiliza la política de seguridad`ELBSecurityPolicy-FS-2018-06`.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
```

```
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Para ver las políticas de seguridad utilizadas por un oyente mediante la CLI

Utilice el comando describe-listeners con el de su oyente. `arn`

```
aws elbv2 describe-listeners \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para ver la configuración de una política de seguridad compatible con FS mediante la CLI

Utilice el comando describe-ssl-policies con cualquier política de seguridad compatible con FS.

En el ejemplo se utiliza la política de seguridad. `ELBSecurityPolicy-FS-2018-06`

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-FS-2018-06
```

TLS 1.0 - 1.2

En la siguiente tabla se describen los protocolos y cifrados TLS compatibles con las políticas de seguridad de TLS 1.0-1.2 disponibles.

Nota: Se ha eliminado el `ELBSecurityPolicy-` prefijo de los nombres de las políticas de la fila de políticas de seguridad.

Ejemplo: La política de seguridad `ELBSecurityPolicy-TLS-1-2-Ext-2018-06` se muestra como`TLS-1-2-Ext-2018-06`.

Políticas de seguridad	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocolos TLS					

Políticas de seguridad	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocolo-TLSv1	✓				✓
Protocolo-TLSv1.1	✓			✓	✓
Protocolo-TLSv1.2	✓	✓	✓	✓	✓
Cifrados TLS					
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓	✓	✓	✓

Políticas de seguridad	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
ECDHE-ECDSA-AES128-SHA	✓	✓		✓	✓
ECDHE-RSA-AES128-SHA	✓	✓		✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓	✓		✓	✓

Políticas de seguridad	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
ECDHE-ECDSA-AES256-SHA	✓	✓		✓	✓
AES128-GCM-SHA256	✓	✓	✓	✓	✓
AES128-SHA256	✓	✓	✓	✓	✓
AES128-SHA	✓	✓		✓	✓
AES256-GCM-SHA384	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓
DES-CBC3-SHA					✓

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

Para crear un agente de escucha HTTPS que utilice una política TLS 1.0-1.2 mediante la CLI

Use el comando create-listener con cualquier política de seguridad compatible con TLS 1.0-1.2.

En el ejemplo se usa la política de seguridad. `ELBSecurityPolicy-2016-08`

```
aws elbv2 create-listener --name my-listener \
--protocol HTTPS --port 443 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Para modificar un agente de escucha HTTPS para que utilice una política TLS 1.0-1.2 mediante la CLI

Use el comando modify-listener con cualquier política de seguridad compatible con TLS 1.0-1.2.

En el ejemplo se usa la política de seguridad. `ELBSecurityPolicy-2016-08`

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-2016-08
```

Para ver las políticas de seguridad utilizadas por un oyente mediante la CLI

Utilice el comando describe-listeners con el de su oyente. `arn`

```
aws elbv2 describe-listeners \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Para ver la configuración de una política de seguridad de TLS 1.0-1.2 mediante la CLI

Utilice el comando describe-ssl-policies con cualquier política de seguridad compatible con TLS 1.0-1.2.

En el ejemplo se usa `ELBSecurityPolicy-2016-08` la política de seguridad.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-2016-08
```

Agregar un oyente HTTPS

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

Requisitos previos

- Para crear un oyente HTTPS, debe especificar un certificado y una política de seguridad. El equilibrador de carga usará el certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de direccionarlas a los destinos. El equilibrador de carga utiliza la política de seguridad para negociar conexiones SSL con los clientes.
- Para añadir una acción de reenvío a la regla predeterminada del oyente, debe especificar un grupo de destino disponible. Para obtener más información, consulte Crear un grupo de destino..
- Puede especificar el mismo grupo de destino en varios oyentes, pero estos deben pertenecer al mismo equilibrador de carga. Para usar un grupo de destino con un equilibrador de carga, debe comprobar que un oyente no lo use para ningún otro equilibrador de carga.

Para agregar un oyente HTTPS mediante la consola

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

   - Reenviar a los grupos de destino: seleccione uno o más grupos de destino a los que reenviar el tráfico. Para añadir grupos de destino, seleccione Añadir grupo de destino. Si utiliza más de un grupo de destino, seleccione una ponderación para cada uno y revise el porcentaje asociado. Debe habilitar la persistencia a nivel de grupo en una regla, si se activó la persistencia en uno o más de los grupos de destino.

- Redirigir a la URL: especifique la URL a la que se redirigirán las solicitudes de los clientes. Esto se puede hacer al introducir cada parte por separado en la pestaña partes de la URI o al ingrsear la dirección completa en la pestaña URL completa. Puede configurar las acciones de redirección como temporales (HTTP 302) o permanentes (HTTP 301), en función de sus necesidades para Código de estado.
- Devolver una respuesta fija: especifique el código de respuesta que se devolverá a las solicitudes de los clientes rechazadas. Además, puede especificar el tipo de contenido y el cuerpo de la respuesta, pero no son obligatorios.

8. Para la política de seguridad, se recomienda utilizar siempre la política de seguridad predefinida más reciente.
9. En Certificado SSL/TLS predeterminado están disponibles las siguientes opciones:

   - Si creó o importó un certificado utilizando AWS Certificate Manager, seleccione De ACM y, a continuación, seleccione el certificado de 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 Certificate Chain (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.

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

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

    Si selecciona Verificar con Trust Store:

    - De forma predeterminada, se rechazan las conexiones con certificados de cliente caducados. Para cambiar este comportamiento, expanda la configuración avanzada de mTLS y, en Vencimiento de los certificados de cliente, seleccione Permitir certificados de cliente caducados.

- En Almacén de confianza, selecciona un almacén de confianza existente o elige Nuevo almacén de confianza.
  - Si ha elegido un nuevo almacén de confianza, proporcione un nombre de almacén de confianza, la ubicación de la autoridad de certificación URI de S3 y, si lo desea, una ubicación en la lista de revocaciones de certificados URI de S3.

11. Seleccione Guardar.

Para añadir un agente de escucha HTTPS mediante el AWS CLI

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

Reglas del oyente del equilibrador de carga de aplicaciones

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

Cada regla consta de una prioridad, una o más acciones y una o más condiciones. Para obtener más información, consulte Reglas del oyente.

Requisitos

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

Agregar una regla

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

Para agregar una regla a través de la consola

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

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

      En la pestaña Reglas, seleccione Añadir regla.

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

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

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

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

     128 caracteres como máximo. No distingue entre mayúsculas y minúsculas. Los caracteres permitidos son a-z, 0-9; los siguientes caracteres especiales: -_.; y caracteres comodín (* y?).
   - Ruta: defina la ruta. Por ejemplo: `/item/*` . Elija Confirmar para guardar la condición.

     128 caracteres como máximo. Distingue mayúsculas de minúsculas. Los caracteres permitidos son letras a-z, A-Z, números 0-9; los siguientes caracteres especiales: _-.$/~"'@; &; y caracteres comodín (* y ?).
   - Método de solicitud HTTP: defina el método de solicitud HTTP. Elija Confirmar para guardar la condición.

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

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

  Se permiten CIDR tanto IPv4 como IPv6. No se admite el uso de comodines.

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

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

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

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

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

    - Reenviar a los grupos de destino: elija uno o más grupos de destino a los que reenviar el tráfico. Para añadir grupos de destino, seleccione Añadir grupo de destino. Si utiliza más de un grupo de destino, seleccione una ponderación para cada uno y revise el porcentaje asociado. Debe habilitar la persistencia a nivel de grupo en una regla, si se activó la persistencia en uno o más de los grupos de destino.
    - Redirigir a la URL: especifique la URL a la que se redirigirán las solicitudes de los clientes. Esto se puede hacer al introducir cada parte por separado en la pestaña partes de la URI o

al ingrsear la dirección completa en la pestaña URL completa. Puede configurar las acciones de redirección como temporales (HTTP 302) o permanentes (HTTP 301), en función de sus necesidades para Código de estado.

- Devolver una respuesta fija: especifique el código de respuesta que se devolverá a las solicitudes de los clientes rechazadas. Además, puede especificar el tipo de contenido y el cuerpo de la respuesta, pero no son obligatorios.

11. Elija Siguiente.
12. Especifique la prioridad de la regla introduciendo un valor entre 1 y 50000.
13. Elija Siguiente.
14. Revise todos los detalles y los ajustes configurados actualmente para la nueva regla. Una vez que esté satisfecho con la configuración, seleccione Crear.

Para añadir una regla mediante el AWS CLI

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

Editar una regla

Puede editar la acción y las condiciones de una regla en cualquier momento. Las actualizaciones de reglas no tienen efecto inmediatamente, por lo que las solicitudes pueden direccionarse utilizando la configuración de reglas anterior durante un breve periodo de tiempo después de actualizar una regla. Todas las solicitudes en tránsito están completadas.

Para editar una regla a través de la consola

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

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

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

Elija Acciones y, a continuación, Editar.

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

Elija Acciones y, a continuación, Editar.

5. Modifique el nombre y las etiquetas según sea necesario. Para agregar otras etiquetas, elija Agregar etiqueta adicional.
6. Elija Siguiente.
7. Modifique las condiciones según sea necesario. Puede añadir, editar una condición existente o eliminarla.
8. Elija Siguiente.
9. Modifique las acciones según sea necesario.
10. Elija Siguiente.
11. Modifique la prioridad de la regla según sea necesario. Puede introducir un valor entre 1 y 50000.
12. Elija Siguiente.
13. Revisa todos los detalles y los ajustes actualizados configurados para tu regla. Cuando esté satisfecho con sus selecciones, elija Guardar cambios.

Para editar una regla mediante AWS CLI

Utilice el comando modify-rule.

Actualizar la prioridad de una regla

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

Para actualizar la prioridad de las reglas mediante la consola

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

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

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

      i. Seleccione Acciones y, a continuación, Volver a priorizar las reglas.

      ii. En la pestaña Reglas, en la sección Reglas de oyente, seleccione Acciones y, a continuación, Cambiar la prioridad de las reglas.

   b. Seleccionar el oyente.

      - Seleccione Administrar reglas y, a continuación, Cambiar la prioridad de las reglas

5. En la sección Reglas de oyente, la columna Prioridad muestra la prioridad de las reglas actuales. Puede actualizar la prioridad de una regla introduciendo un valor comprendido entre 1 y 50000.
6. Cuando los cambios le parezcan finalizados, seleccione Guardar cambios.

Para actualizar las prioridades de las reglas mediante AWS CLI

Utilice el comando set-rule-priorities.

Eliminar una regla

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

Para eliminar una regla a través de la consola

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

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

      i. Seleccione la regla que desea eliminar.

      ii. Seleccione Acciones, y luego Eliminar regla.

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

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

   i. Seleccione Acciones, y luego Eliminar regla.

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

Para eliminar una regla mediante el AWS CLI

Utilice el comando delete-rule.

Actualizar un oyente HTTPS para el equilibrador de carga de aplicaciones

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

Tareas

- Reemplazar el certificado predeterminado
- Añadir certificados a la lista de certificados
- Quitar certificados de la lista de certificados
- Actualizar la política de seguridad

Reemplazar el certificado predeterminado

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

Para cambiar el certificado predeterminado utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, elija el texto de la columna Protocolo:Puerto para abrir la página de detalles del oyente.
5. En la pestaña Certificados, elija Cambiar el valor predeterminado.

6. En la tabla de certificados de ACM e IAM, seleccione un nuevo certificado predeterminado.
7. Seleccione Guardar como predeterminado.

Para cambiar el certificado predeterminado mediante AWS CLI

Utilice el comando modify-oyente.

Añadir certificados a la lista de certificados

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

Para cambiar el certificado predeterminado utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, elija el texto de la columna Protocolo:Puerto para abrir la página de detalles del oyente.
5. En la pestaña Certificados, elija Agregar certificado.
6. En la tabla certificados de ACM e IAM, seleccione los certificados que desee añadir y, a continuación, seleccione Incluir como pendientes.
7. Si cuenta con un certificado que no se encuentra administrado por ACM o IAM, elija Importar certificado, complete el formulario y elija Importar.
8. Elija Agregar certificados pendientes.

Para agregar un certificado a la lista de certificados mediante el AWS CLI

Utilice el comando add-oyente-certificates.

Quitar certificados de la lista de certificados

Puede quitar certificados de la lista de certificados para su oyente HTTPS utilizando el siguiente procedimiento. Para quitar el certificado predeterminado para un oyente HTTPS, consulte Reemplazar el certificado predeterminado.

Para quitar certificados de la lista de certificados utilizando la consola

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

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

Utilice el comando remove-oyente-certificates.

Actualizar la política de seguridad

Cuando crea un oyente HTTPS, puede seleccionar la política de seguridad que mejor se ajuste a sus necesidades. Cuando se agrega una nueva política de seguridad, se puede actualizar el oyente HTTPS para que la utilice. Los equilibradores de carga de aplicaciones no admiten políticas de seguridad personalizadas. Para obtener más información, consulte Políticas de seguridad.

Uso de políticas FIPS en su Application Load Balancer:

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

Para actualizar la política de seguridad a través de la consola

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

Para actualizar la política de seguridad mediante AWS CLI

Utilice el comando modify-oyente.

Autenticación mutua con TLS en Application Load Balancer

La autenticación TLS mutua es una variante de la seguridad de la capa de transporte (TLS). El TLS tradicional establece comunicaciones seguras entre un servidor y un cliente, donde el servidor debe proporcionar su identidad a sus clientes. Con el TLS mutuo, un balanceador de cargas negocia la autenticación mutua entre el cliente y el servidor mientras negocia el TLS. Al usar el TLS mutuo con Application Load Balancer, se simplifica la administración de la autenticación y se reduce la carga de las aplicaciones.

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

El TLS mutuo para los balanceadores de carga de aplicaciones ofrece las dos opciones siguientes para validar los certificados de cliente X.509v3:

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

- Transferencia TLS mutua: cuando se utiliza el modo de transferencia TLS mutua, Application Load Balancer envía toda la cadena de certificados del cliente al destino mediante encabezados HTTP. Luego, al usar la cadena de certificados del cliente, puede implementar la lógica de autenticación y autorización correspondiente en su aplicación.
- Verificación TLS mutua: cuando se usa el modo de verificación TLS mutua, Application Load Balancer realiza la autenticación del certificado de cliente X.509 para los clientes cuando un balanceador de carga negocia las conexiones TLS.

Para empezar a utilizar el TLS mutuo en Application Load Balancer mediante la transferencia directa, solo tiene que configurar el listener para que acepte los certificados de los clientes. Para usar el TLS mutuo con la verificación, debe hacer lo siguiente:

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

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

Antes de empezar a configurar el TLS mutuo en su Application Load Balancer

Antes de empezar a configurar el TLS mutuo en su Application Load Balancer, tenga en cuenta lo siguiente:

Cuotas

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

Para obtener más información, consulte Cuotas para sus balanceadores de carga de aplicaciones.

Requisitos de los certificados

Los balanceadores de carga de aplicaciones admiten lo siguiente para los certificados que se utilizan con la autenticación TLS mutua:

- Certificado compatible: X.509v3
- Claves públicas compatibles: RSA 2K — 8K o ECDSA secp256r1, secp384r1, secp521r1
- Algoritmos de firma compatibles: SHA256, 384, 512 con RSA/SHA256, 384, 512 con EC/SHA256.384.512 hash con RSASSA-PSS con MGF1

Paquetes de certificados de CA

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

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

Pedido de certificado para la transferencia

Cuando se utiliza la transferencia TLS mutua, Application Load Balancer inserta encabezados para presentar la cadena de certificados del cliente a los destinos del backend. El orden de presentación comienza con los certificados de hoja y termina con el certificado raíz.

Reanudación de la sesión

No se admite la reanudación de la sesión cuando se utilizan los modos de verificación o transferencia TLS mutua con un Application Load Balancer.

Encabezados HTTP

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

Archivos de certificados de CA

Los archivos de certificados de CA deben cumplir los siguientes requisitos:

- El archivo de certificado debe usar el formato PEM (Privacy Enhanced Mail).

- El contenido del certificado debe estar dentro de los `-----END CERTIFICATE-----` límites `-----BEGIN CERTIFICATE-----` y.
- Los comentarios deben ir precedidos de un # carácter.
- No puede haber líneas en blanco.

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

```
# comments

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

Ejemplos de certificados que se aceptan (válidos):

1. Certificado único (codificado en PEM):

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

2. Varios certificados (codificados en PEM):

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

Encabezados HTTP y TLS mutuo

En esta sección, se describen los encabezados HTTP que los balanceadores de carga de aplicaciones utilizan para enviar la información de los certificados cuando negocian conexiones con clientes que utilizan un TLS mutuo. `X-Amzn-Mtls`Los encabezados específicos que utiliza Application Load Balancer dependen del modo TLS mutuo que haya especificado: modo de transferencia o modo de verificación.

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

Encabezado HTTP para el modo de acceso directo

Para el TLS mutuo en modo de transferencia, los balanceadores de carga de aplicaciones utilizan el siguiente encabezado.

X-Aman-Mtls-Clientcert

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

Ejemplo de contenido del encabezado:

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

Cabeceras HTTP para el modo de verificación

Para el TLS mutuo en modo de verificación, los balanceadores de carga de aplicaciones utilizan los siguientes encabezados.

Número de serie X-Amzn-Mtls-Clientcert

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

Ejemplo de contenido del encabezado:

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

X-Amzn-Mtls-Clientcert-Issuer

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

Ejemplo de contenido del encabezado:

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

X-Amzn-Mtls-Clientcert-Subject

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

Ejemplo de contenido del encabezado:

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

X-Amzn-Mtls-Clientcert-Validity

Este encabezado contiene un formato ISO8601 de la fecha y. `notBefore` `notAfter`

Ejemplo de contenido del encabezado:

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

X-Amzn-Mtls-Clientcert-Leaf

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

Ejemplo de contenido del encabezado:

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

Configuración del TLS mutuo en un Application Load Balancer

Esta sección incluye los procedimientos para configurar el modo de verificación TLS mutua para la autenticación en los balanceadores de carga de aplicaciones.

Para usar el modo de transferencia TLS mutua, solo necesita configurar el listener para que acepte los certificados de los clientes. Cuando utiliza la transferencia TLS mutua, Application Load Balancer envía toda la cadena de certificados del cliente al destino mediante encabezados HTTP, lo que le permite implementar la lógica de autenticación y autorización correspondiente en la aplicación. Para obtener más información, consulte Create an HTTPS listener for your Application Load Balancer (Crear un oyente HTTPS para el equilibrador de carga de aplicación).

Cuando se usa el TLS mutuo en el modo de verificación, Application Load Balancer realiza la autenticación del certificado de cliente X.509 para los clientes cuando un balanceador de carga negocia las conexiones TLS.

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

- Cree un nuevo recurso de almacén de confianza.
- Cargue su paquete de entidades de certificación (CA) y, si lo desea, las listas de revocación.

- Adjunte el almacén de confianza al agente de escucha que está configurado para verificar los certificados de los clientes.

Siga los procedimientos de esta sección para configurar el modo de verificación TLS mutua en su Application Load Balancer en. AWS Management Console Para configurar el TLS mutuo mediante operaciones de API en lugar de la consola, consulta la Guía de referencia de la API Application Load Balancer.

Tareas

- Cree un almacén de confianza
- Asocia un almacén de confianza
- Consulta los detalles del almacén de confianza
- Modifica un almacén de confianza
- Eliminar un almacén de confianza

Cree un almacén de confianza

Hay tres formas de crear un almacén de confianza: al crear un Application Load Balancer, al crear un agente de escucha seguro y mediante la consola de Trust Store. Al añadir un almacén de confianza al crear un equilibrador de carga o un agente de escucha, el almacén de confianza se asocia automáticamente al nuevo agente de escucha. Al crear un almacén de confianza mediante la consola de Trust Store, debe asociarlo usted mismo a un agente de escucha.

En esta sección se describe la creación de un almacén de confianza mediante la consola de Trust Store, pero los pasos que se siguen al crear un Application Load Balancer o un listener son los mismos. Para obtener más información, consulte Configurar un equilibrador de carga y un agente de escucha y Añadir un agente de escucha HTTPS.

Requisitos previos:

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

Para crear un almacén de confianza mediante la consola

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

2. En el panel de navegación, elija Trust Stores.
3. Seleccione Crear un almacén de confianza.
4. Configuración del almacén de confianza

   a. En Nombre del almacén de confianza, introduzca un nombre para su almacén de confianza.

   b. Para el paquete de autoridad de certificación, introduzca la ruta de Amazon S3 al paquete de certificados ca que desee que utilice su almacén de confianza.

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

5. En el caso de las revocaciones, si lo desea, puede añadir una lista de certificados revocados a su almacén de confianza.

   - En Lista de revocaciones de certificados, introduzca la ruta de Amazon S3 a la lista de revocación de certificados que desee que utilice su almacén de confianza.

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

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

Asocia un almacén de confianza

Tras crear un almacén de confianza, debe asociarlo a un agente de escucha para que Application Load Balancer pueda empezar a utilizar el almacén de confianza. Solo puede tener un almacén de confianza asociado a cada uno de sus agentes de escucha seguros, pero un almacén de confianza puede estar asociado a varios agentes de escucha.

En esta sección se describe la asociación de un almacén de confianza a un oyente existente. Como alternativa, puede asociar un almacén de confianza al crear un Application Load Balancer o un listener. Para obtener más información, consulte Configurar un equilibrador de carga y un agente de escucha y Añadir un agente de escucha HTTPS.

Para asociar un almacén de confianza mediante la consola

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

2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el balanceador de cargas para ver su página de detalles.
4. En la pestaña Listeners and rules, selecciona el enlace de la columna Protocol:Port para abrir la página de detalles del listener seguro.
5. En la pestaña Seguridad, seleccione Editar la configuración del agente de escucha seguro.
6. (Opcional) Si el TLS mutuo no está habilitado, seleccione Autenticación mutua (mTLS) en Gestión de certificados de cliente y, a continuación, elija Verificar con un almacén de confianza.
7. En Almacén de confianza, elija el almacén de confianza que ha creado.
8. Elija Guardar cambios.

Consulta los detalles del almacén de confianza

Paquetes de certificados de CA

El paquete de certificados de CA es un componente obligatorio del almacén de confianza. Es un conjunto de certificados raíz e intermedios de confianza que han sido validados por una autoridad de certificación. Estos certificados validados garantizan que el cliente pueda confiar en que el certificado que se presenta es propiedad del balanceador de cargas.

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

Vea un paquete de certificados de CA

Para ver un paquete de certificados de CA mediante la consola

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

Listas de revocación de certificados

Si lo desea, puede crear una lista de revocaciones de certificados para un almacén de confianza. Las autoridades de certificación publican las listas de revocación y contienen datos de los certificados

que se han revocado. Los balanceadores de carga de aplicaciones solo admiten listas de revocación de certificados en formato PEM.

Cuando se agrega una lista de revocación de certificados a un almacén de confianza, se le asigna un identificador de revocación. Los ID de revocación aumentan con cada lista de revocación que se añade al almacén de confianza y no se pueden cambiar. Si se elimina una lista de revocación de certificados de un almacén de confianza, su identificador de revocación también se elimina y no se reutiliza mientras dure el almacén de confianza.

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

Ver una lista de revocaciones de certificados

Para ver una lista de revocaciones mediante la consola

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

Modifica un almacén de confianza

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

Sustituya un paquete de certificados de CA

Para reemplazar un paquete de certificados de CA mediante la consola

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

3. Seleccione el almacén de confianza para ver la página de detalles.
4. Seleccione Acciones y, a continuación, Sustituya el paquete CA.
5. En la página Reemplazar paquete de CA, en Paquete de autoridad de certificación, introduzca la ubicación de Amazon S3 del paquete de CA deseado.
6. (Opcional) Utilice la versión de objeto para seleccionar una versión anterior de la lista de revocaciones de certificados. De lo contrario, se utilizará la versión actual.
7. Seleccione Reemplazar el paquete CA.

Agregue una lista de revocaciones de certificados

Para añadir una lista de revocaciones mediante la consola

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

Eliminar una lista de revocaciones de certificados

Para eliminar una lista de revocaciones mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Trust Stores.
3. Seleccione el almacén de confianza para ver la página de detalles.
4. En la pestaña Listas de revocación de certificados, seleccione Acciones y, a continuación, Eliminar lista de revocaciones.
5. Confirme la eliminación escribiendo. `confirm`
6. Seleccione Eliminar.

Eliminar un almacén de confianza

Cuando ya no utilices un almacén de confianza, puedes eliminarlo.

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

Para eliminar un almacén de confianza mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Trust Stores.
3. Seleccione el almacén de confianza para ver su página de detalles.
4. Selecciona Acciones y, a continuación, Eliminar el almacén de confianza.
5. Confirme la eliminación escribiendo`confirm`.
6. Selecciona Eliminar

Registros de conexión para los balanceadores de carga de aplicaciones

Elastic Load Balancing proporciona registros de conexión que capturan los atributos de las solicitudes enviadas a los balanceadores de carga de aplicaciones. Los registros de conexión contienen información como la dirección IP y el puerto del cliente, la información del certificado del cliente, los resultados de la conexión y los cifrados TLS que se utilizan. Estos registros de conexión se pueden usar luego para revisar los patrones de solicitudes y otras tendencias.

Para obtener más información sobre los registros de conexión, consulte Registros de conexión para su Application Load Balancer

Autenticación de usuarios mediante un Equilibrador de carga de aplicación

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

Se admiten los siguientes casos de uso:

- Autenticar a los usuarios a través de un proveedor de identidad (IdP) compatible con OpenID Connect (OIDC).

- Autentique a los usuarios a través de redes sociales IdPs, como Amazon o Google FaceBook, a través de los grupos de usuarios compatibles con Amazon Cognito.
- Autentique a los usuarios mediante identidades corporativas, mediante SAML, OpenID Connect (OIDC) u OAuth, a través de los grupos de usuarios compatibles con Amazon Cognito.

Preparativos para usar un IdP compatible con OIDC

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

- Cree una nueva aplicación OIDC en su IdP. El DNS del IdP debe poder resolverse públicamente.
- Debe configurar un ID de cliente y un secreto de cliente.
- Obtenga los siguientes puntos de enlace publicados por el IdP: autorización, token e información de usuario. Puede localizar esta información en la configuración.
- Los certificados de los puntos de conexión del IdP deben ser emitidos por una autoridad de certificación pública de confianza.
- Las entradas de DNS de los puntos de conexión deben poder resolverse públicamente, incluso si se resuelven en direcciones IP privadas.
- Permita una de las siguientes URL de redirección en su aplicación de IdP, sea cual sea la que utilicen sus usuarios, donde DNS es el nombre de dominio del equilibrador de carga y CNAME es el alias DNS de su aplicación:
  - https://*DNS*/oauth2/idpresponse
  - https://*CNAME*/oauth2/idpresponse

Preparación para usar Amazon Cognito

Regiones disponibles

La integración de Amazon Cognito para los balanceadores de carga de aplicaciones está disponible en las siguientes regiones:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Norte de California)
- Oeste de EE. UU. (Oregón)

- Canadá (centro)
- Europa (Estocolmo)
- Europa (Milán)
- Europa (Fráncfort)
- Europa (Zúrich)
- Europa (Irlanda)
- Europa (Londres)
- Europa (París)
- América del Sur (São Paulo)
- Asia-Pacífico (Tokio)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Yakarta)
- Medio Oriente (EAU)
- Medio Oriente (Baréin)
- África (Ciudad del Cabo)
- Israel (Tel Aviv)

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

- Cree un grupo de usuarios. Para obtener más información, consulte Grupos de usuarios de Amazon Cognito en la Guía para desarrolladores de Amazon Cognito.
- Cree un cliente del grupo de usuarios. Debe configurar el cliente para que genere un secreto de cliente, utilice el flujo de concesión de código y admita los mismos ámbitos de OAuth que utiliza el equilibrador de carga. Para obtener más información, consulte Configuración de un cliente de aplicación de grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.
- Cree un dominio de grupo de usuarios. Para obtener más información, consulte Agregar un nombre de dominio para el grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

- Compruebe que el ámbito solicitado devuelve un token de ID. Por ejemplo, el ámbito predeterminado, `openid`, devuelve un token de ID pero el ámbito `aws.cognito.signin.user.admin` no.

  Nota: Los balanceadores de carga de aplicaciones no admiten los tokens de acceso personalizados emitidos por Amazon Cognito. Para obtener más información, consulte la generación previa del token en la Guía para desarrolladores de Amazon Cognito.
- Para federarse con un IdP social o corporativo, habilite el IdP en la sección de federación. Para obtener más información, consulte Añadir inicio de sesión de redes sociales a un grupo de usuarios o Añadir inicio de sesión con un IdP SAML a un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.
- Permita las siguientes URL de redirección en el campo de URL de devolución de llamada para Amazon Cognito, donde DNS es el nombre de dominio del equilibrador de carga y CNAME es el alias DNS de su aplicación (si utiliza uno):
  - https://*DNS*/oauth2/idpresponse
  - https://*CNAME*/oauth2/idpresponse
- Permita el dominio del grupo de usuarios en la URL de devolución de llamada de la aplicación de IdP. Utilice el formato de su IdP. Por ejemplo:
  - https://*domain-prefix*.auth.*region*.amazoncognito.com/saml2/idpresponse
  - https://*dominio-de-grupo-de-usuarios*/oauth2/idpresponse

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

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

Prepárate para usar Amazon CloudFront

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

- Reenviar los encabezados de las solicitudes (todos): garantiza que CloudFront no se almacenen en caché las respuestas de las solicitudes autenticadas. Esto evita que se sirvan desde la caché después de que venza la sesión de autenticación. Como alternativa, para reducir este

riesgo mientras el almacenamiento en caché está activado, los propietarios de una CloudFront distribución pueden configurar el valor time-to-live (TTL) para que caduque antes de que caduque la cookie de autenticación.

- Reenvío y almacenamiento en caché de cadenas de consulta (todos): garantiza que el equilibrador de carga tenga acceso a los parámetros de la cadena de consulta necesarios para autenticar al usuario con el IdP.
- Reenvío de cookies (todas): garantiza que se CloudFront reenvíen todas las cookies de autenticación al balanceador de cargas.

Configuración de la autenticación de usuarios

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

El equilibrador de carga envía una cookie de sesión al cliente para mantener el estado de autenticación. Esta cookie siempre contiene el atributo `secure`, porque la autenticación del usuario requiere un oyente HTTPS. Esta cookie contiene el atributo `SameSite=None` con solicitudes CORS (intercambio de recursos de varios orígenes).

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

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

De forma predeterminada, el campo `SessionTimeout` está configurado en 7 días. Si desea sesiones más cortas, puede configurar un tiempo de espera de sesión de tan solo 1 segundo. Para obtener más información, consulte Tiempo de espera de la sesión.

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

- Aplicaciones que requieren que el usuario inicie sesión mediante una identidad social o corporativa: se admite mediante la opción predeterminada `authenticate`. Si el usuario no ha

iniciado sesión, el equilibrador de carga redirige la solicitud al punto de conexión de autorización de IdP y el IdP le pide al usuario que inicie sesión utilizando su interfaz de usuario.

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

El equilibrador de carga debe poder comunicarse con el punto de conexión de token de IdP (`TokenEndpoint`) y el punto de conexión de información de usuario de IdP (`UserInfoEndpoint`). Los balanceadores de carga de aplicaciones solo admiten IPv4 cuando se comunican con estos puntos finales. Si su IdP usa direcciones públicas, asegúrese de que los grupos de seguridad del balanceador de cargas y las ACL de red de la VPC permitan el acceso a los puntos finales. Cuando se utiliza un balanceador de cargas interno o el tipo de dirección IP`dualstack-without-public-ipv4`, una puerta de enlace NAT puede permitir que el balanceador de cargas se comunique con los puntos finales. Para obtener más información, consulte Información básica de puertas de enlace NAT en la Guía del usuario de Amazon VPC.

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

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

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

```
[{
    "Type": "authenticate-oidc",
    "AuthenticateOidcConfig": {
```

```
        "Issuer": "https://idp-issuer.com",
        "AuthorizationEndpoint": "https://authorization-endpoint.com",
        "TokenEndpoint": "https://token-endpoint.com",
        "UserInfoEndpoint": "https://user-info-endpoint.com",
        "ClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "ClientSecret": "1234567890123456789012345678 90",
        "SessionCookieName": "my-cookie",
        "SessionTimeout": 3600,
        "Scope": "email",
        "AuthenticationRequestExtraParams": {
            "display": "page",
            "prompt": "login"
        },
        "OnUnauthenticatedRequest": "deny"
    },
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

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

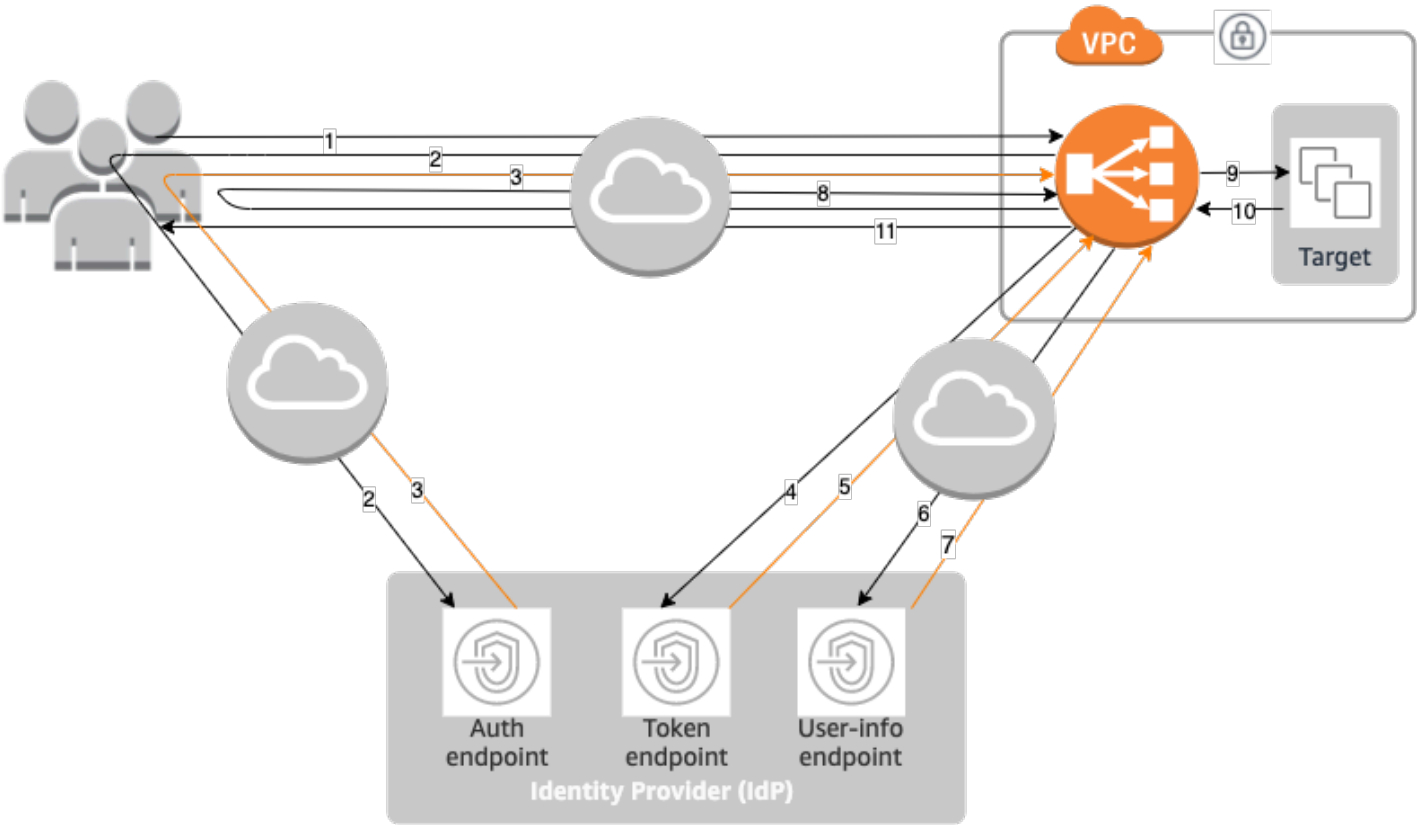
```
[{
    "Type": "authenticate-cognito",
    "AuthenticateCognitoConfig": {
        "UserPoolArn": "arn:aws:cognito-idp:region-code:account-id:userpool/user-pool-
id",
        "UserPoolClientId": "abcdefghijklmnopqrstuvwxyz123456789",
        "UserPoolDomain": "userPoolDomain1",
        "SessionCookieName":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

```
    "Order": 1
},
{
    "Type": "forward",
    "TargetGroupArn": "arn:aws:elasticloadbalancing:region-code:account-
id:targetgroup/target-group-name/target-group-id",
    "Order": 2
}]
```

Para obtener más información, consulte Reglas del oyente.

Flujo de autenticación

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



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

1. El usuario envía una solicitud HTTPS a un sitio web alojado detrás de un Equilibrador de carga de aplicación. Cuando se cumplen las condiciones de una regla con una acción de

autenticación, el equilibrador de carga comprueba si hay una cookie de sesión de autenticación en los encabezados de solicitudes.

2. Si la cookie no está presente, el equilibrador de carga redirige al usuario al punto de conexión de autorización de IdP para que el IdP pueda autenticarlo.
3. Después de autenticar al usuario, el IdP lo redirige al equilibrador de carga con un código de concesión de autorización.
4. El equilibrador de carga presenta el código de concesión de autorización al punto de conexión del token de IdP.
5. Al recibir un código de concesión de autorización válido, el IdP proporciona el token de identificación y el token de acceso al Equilibrador de carga de aplicación.
6. A continuación, el Equilibrador de carga de aplicación envía el token de acceso al punto de conexión de información del usuario.
7. El punto de conexión de información del usuario intercambia el token de acceso por las solicitudes de los usuarios.
8. El Equilibrador de carga de aplicación redirige al usuario con la cookie de sesión de autenticación de `AWSELB` al URI original. Debido a que la mayoría de los navegadores limitan una cookie a 4 KB de tamaño, el equilibrador de carga fragmenta una cookie de más de 4 KB en varias cookies. Si el tamaño total de las notificaciones de usuario y el token de acceso recibido del IdP es superior a 11 KB, el equilibrador de carga devuelve un error HTTP 500 al cliente y aumenta la métrica `ELBAuthUserClaimsSizeExceeded`.
9. El Equilibrador de carga de aplicación valida la cookie y reenvía la información del usuario a los destinos del conjunto de encabezados HTTP de `X-AMZN-OIDC-*`. Para obtener más información, consulte Codificación de las notificaciones de usuario y verificación de firmas.
10. El destino envía una respuesta al Equilibrador de carga de aplicación.
11. El Equilibrador de carga de aplicación envía la respuesta final al usuario.

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

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

Si el IdP proporciona un token de actualización válido en el token de ID, el equilibrador de carga lo guarda y lo utiliza para actualizar las notificaciones de usuario cada vez que venza el token de acceso, hasta que se agote la sesión o hasta que se produzca un error en la actualización del IdP. Si el usuario cierra la sesión, se produce un error en la actualización y el equilibrador de carga redirige al usuario al punto de conexión de autorización de IdP. De este modo, el equilibrador de carga puede dejar de funcionar después de que el usuario cierre la sesión. Para obtener más información, consulte Tiempo de espera de la sesión.

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

Codificación de las notificaciones de usuario y verificación de firmas

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

El equilibrador de carga añade los siguientes encabezados HTTP:

`x-amzn-oidc-accesstoken`

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

`x-amzn-oidc-identity`

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

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

`x-amzn-oidc-data`

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

Los tokens de acceso y las reclamaciones de los usuarios son diferentes de los tokens de identificación. Los tokens de acceso y las reclamaciones de usuario solo permiten el acceso a los recursos del servidor, mientras que los tokens contienen información adicional para autenticar a un usuario. El Application Load Balancer crea un nuevo token de acceso al autenticar a un usuario y solo pasa los tokens de acceso y los reclamos al backend; sin embargo, no pasa la información del token de ID.

Estos tokens siguen el formato JWT, pero no son tokens de ID. El formato JWT incluye un encabezado, una carga y una firma que tienen codificación de URL en base64 e incluyen caracteres de relleno al final. Un Equilibrador de carga de aplicación usa ES256 (ECDSA usa P-256 y SHA256) para generar la firma JWT.

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

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

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

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

Dado que el equilibrador de carga no cifra las notificaciones de usuario, le recomendamos que configure el grupo de destino para que utilice HTTPS. Si configura el grupo de destino para que utilice HTTP, asegúrese de restringir el tráfico a su equilibrador de carga mediante grupos de seguridad.

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

Para obtener la clave pública, obtenga el ID de clave del encabezado JWT y utilícelo para buscar la clave pública desde el siguiente punto de conexión regional. El punto de conexión de cada región de AWS es el siguiente:

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

AWS GovCloud (US) En efecto, los puntos finales son los siguientes:

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

El siguiente ejemplo muestra cómo obtener la identificación de clave, la clave pública y la carga en Python 3.x:

```
import jwt
import requests
import base64
import json

# Step 1: Validate the signer
expected_alb_arn = 'arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/
app/load-balancer-name/load-balancer-id'

encoded_jwt = headers.dict['x-amzn-oidc-data']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_jwt_headers = decoded_jwt_headers.decode("utf-8")
decoded_json = json.loads(decoded_jwt_headers)
received_alb_arn = decoded_json['signer']

assert expected_alb_arn == received_alb_arn, "Invalid Signer"

# Step 2: Get the key id from JWT headers (the kid field)
kid = decoded_json['kid']

# Step 3: Get the public key from regional endpoint
url = 'https://public-keys.auth.elb.' + region + '.amazonaws.com/' + kid
```

```
req = requests.get(url)
pub_key = req.text

# Step 4: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES256'])
```

El siguiente ejemplo muestra cómo obtener la identificación de clave, la clave pública y la carga en Python 2.7:

```
import jwt
import requests
import base64
import json

# Step 1: Validate the signer
expected_alb_arn = 'arn:aws:elasticloadbalancing:region-code:account-id:loadbalancer/
app/load-balancer-name/load-balancer-id'

encoded_jwt = headers.dict['x-amzn-oidc-data']
jwt_headers = encoded_jwt.split('.')[0]
decoded_jwt_headers = base64.b64decode(jwt_headers)
decoded_json = json.loads(decoded_jwt_headers)
received_alb_arn = decoded_json['signer']

assert expected_alb_arn == received_alb_arn, "Invalid Signer"

# Step 2: Get the key id from JWT headers (the kid field)
kid = decoded_json['kid']

# Step 3: Get the public key from regional endpoint
url = 'https://public-keys.auth.elb.' + region + '.amazonaws.com/' + kid
req = requests.get(url)
pub_key = req.text

# Step 4: Get the payload
payload = jwt.decode(encoded_jwt, pub_key, algorithms=['ES256'])
```

Consideraciones

- Estos ejemplos no abarcan cómo validar la firma del emisor con la firma en el token.
- Las bibliotecas estándar no son compatibles con el relleno que se incluye en el token de autenticación de Equilibrador de carga de aplicación en formato JWT.

Tiempo de espera

Tiempo de espera de la sesión

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

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

Tiempo de espera de inicio de sesión de cliente

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

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

Cierre de sesión de autenticación

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

La página de inicio de cierre de sesión del cliente es una página no autenticada. Esto significa que no puede estar detrás de una regla de Equilibrador de carga de aplicación que requiera autenticación.

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

Encabezados HTTP y balanceadores de tipo equilibrador de carga de aplicaciones

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

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

Encabezados X-Forwarded

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

X-Forwarded-For

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

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

Anexar

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

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

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

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

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

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

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

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

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

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

En el caso de IPv6, tenga en cuenta que cuando el equilibrador de carga añade el `client-ip-address` al encabezado existente, coloca la dirección entre corchetes.

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

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

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

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

Conservar

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

Remove

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

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

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

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

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

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

5. En la sección Configuración del tráfico, en Gestión de paquetes, para Encabezado X-Forwarded-For, elija Añadir (predeterminado), Conservar o Eliminar.
6. Elija Guardar cambios.

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

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

X-Forwarded-Proto

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

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

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

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

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

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

X-Forwarded-Port

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

Etiquetas para sus oyentes y reglas

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

Puede agregar varias etiquetas a cada oyente y regla. Las claves de las etiquetas deben ser únicas para cada oyente y regla. Si agrega una etiqueta con una clave que ya está asociada al oyente y la regla, se actualiza el valor de esa etiqueta.

Cuando ya no necesite una etiqueta, puede eliminarla.

Restricciones

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 127 caracteres Unicode
- Longitud máxima del valor: 255 caracteres Unicode
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Los caracteres permitidos son letras, espacios y números representables en UTF-8, además de los siguientes caracteres especiales: + - = . _ : / @. No utilice espacios iniciales ni finales.
- No utilice el `aws:` prefijo en los nombres o valores de las etiquetas 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.

Actualizar las etiquetas de oyente

Para actualizar las etiquetas de un oyente desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga que contiene el oyente que desea actualizar para abrir su página de detalles.
4. En la pestaña Oyentes y reglas, realice alguna de las siguientes acciones:

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

      En la pestaña Tags (Etiquetas), elija Manage tags (Administrar etiquetas).

b. Seleccione el oyente en el que desea actualizar las etiquetas.

   Seleccione Administrar el oyente y, a continuación, Administrar etiquetas.

c. Seleccione el texto de la columna Etiquetas para abrir la página de detalles del oyente, en la pestaña Etiquetas.

   Elija Administrar etiquetas.

5. En la página Administrar etiquetas, puede hacer lo siguiente:

   a. Para actualizar una etiqueta, ingrese valores nuevos para Clave y Valor.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta nueva y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.

6. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de un oyente mediante el AWS CLI

Utilice los comandos add-tags y remove-tags.

Actualizar las etiquetas de reglas

Para actualizar las etiquetas de una regla desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga que contiene la regla que desea actualizar para abrir su página de detalles.
4. En la pestaña Oyentes y reglas, elija el texto de la columna Protocolo:Puerto del oyente que contiene la regla que desea actualizar, para abrir la página de detalles del oyente.
5. En la página de detalles del oyente, realice una de las siguientes operaciones:

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

      En la página Detalles de la regla, elija Editar.

   b. Seleccione el texto de la columna Etiquetas para la regla que desee actualizar.

      En la ventana emergente de resumen de etiquetas, seleccione Administrar etiquetas.

6. En la página Administrar etiquetas, puede hacer lo siguiente:
   a. Para actualizar una etiqueta, ingrese valores nuevos para Clave y Valor.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta nueva y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.
7. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de una regla mediante el AWS CLI

Utilice los comandos add-tags y remove-tags.

Eliminar un oyente de Equilibrador de carga de aplicación

Puede eliminar un oyente en cualquier momento. Cuando se elimina un equilibrador de carga, se eliminan todos sus oyentes.

Para eliminar un oyente a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el equilibrador de carga.
4. En la pestaña Oyentes y reglas, seleccione la casilla de verificación del oyente y elija Administrar oyente, Eliminar oyente.
5. Cuando se le pida confirmación, ingrese **`confirm`** y elija Eliminar.

Para eliminar un oyente mediante el AWS CLI

Utilice el comando delete-listener.

Grupos de destino para los equilibradores de carga de aplicaciones

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

Cada grupo de destino se utiliza para direccionar solicitudes a uno o varios destinos registrados. Cuando se crea la regla de cada oyente, se especifican un grupo de destino y las condiciones. Cuando se cumple la condición de una regla, el tráfico se reenvía al grupo de destino correspondiente. Puede crear grupos de destino diferentes para los distintos tipos de solicitudes. Por ejemplo, puede crear un grupo de destino para las solicitudes generales y otros grupos de destino para las solicitudes destinadas a los microservicios de la aplicación. Puede usar cada grupo de destino con un solo equilibrador de carga. Para obtener más información, consulte Componentes del Equilibrador de carga de aplicación.

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

Contenido

- Configuración de enrutamiento
- Tipo de destino
- Tipo de dirección IP
- Versión del protocolo
- Destinos registrados
- Atributos del grupo de destino
- Los algoritmos de enrutamiento
- Pesos objetivo automáticos (ATW)

- Retardo de anulación del registro
- Modo de inicio lento
- Crear un grupo de destino.
- Comprobaciones de estado de los grupos de destino
- Equilibrio de carga entre zonas para grupos de destino
- Estado del grupo de destino
- Registro de destinos con el grupo de destino
- Sesiones persistentes para Equilibrador de carga de aplicación
- Funciones de Lambda como destino
- Etiquetas para su grupo de destino
- Eliminación de un grupo de destino

Configuración de enrutamiento

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

Los grupos de destino admiten los siguientes protocolos y puertos:

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

Si un grupo de destino se configura con el protocolo HTTPS o utiliza comprobaciones de estado HTTPS, las conexiones SSL/TLS a los destinos utilizarán la configuración de seguridad de la política `ELBSecurityPolicy-2016-08`. El equilibrador de carga establece conexiones TLS con los destinos mediante certificados que instala en los destinos. El equilibrador de carga no valida estos certificados. Por lo tanto, puede utilizar certificados autofirmados o certificados que hayan caducado. Como el balanceador de cargas y sus objetivos se encuentran en una nube privada virtual (VPC), el tráfico entre el balanceador de cargas y los destinos se autentica a nivel de paquete, por lo que no corre el riesgo man-in-the-middle de sufrir ataques o suplantación de identidad aunque los certificados de los destinos no sean válidos. El tráfico que salga no AWS contará con las mismas protecciones, por lo que es posible que se necesiten medidas adicionales para proteger aún más el tráfico.

Tipo de destino

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

Los tipos de destinos posibles son los siguientes:

`instance`

Los destinos se especifican por ID de instancia.

`ip`

Los destinos son direcciones IP.

`lambda`

El destino es una función de Lambda.

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

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

> **Important**
>
> No puede especificar direcciones IP direccionables públicamente.

Todos los bloques CIDR compatibles le permiten registrar los siguientes destinos en un grupo de destino:

- Instancias en una VPC que está interconectada a la VPC del equilibrador de carga (misma región o región diferente).

- AWS recursos que se pueden direccionar mediante una dirección IP y un puerto (por ejemplo, bases de datos).
- Recursos locales enlazados a AWS través de una conexión VPN Site-to-Site AWS Direct Connect o a una conexión VPN.

> **Note**
>
> En el caso de los equilibradores de carga de aplicaciones implementados en una zona local, los destinos `ip` deben estar en la misma zona local para recibir tráfico.
> Para obtener más información, consulte ¿Qué son las Zonas AWS Locales?

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

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

Puede configurar Amazon Elastic Container Service (Amazon ECS) como destino de Equilibrador de carga de aplicación. Para obtener más información, consulte Creating an Application Load Balancer en la Guía del usuario de Amazon Elastic Container Service para. AWS Fargate

Tipo de dirección IP

Al crear un nuevo grupo de destino, puede seleccionar el tipo de dirección IP de su grupo de destino. Esto controla la versión de IP utilizada para comunicarse con los destinos y comprobar su estado.

Los equilibradores de carga de aplicaciones admiten grupos de destino IPv4 e IPv6. La selección predeterminada es IPv4.

Consideraciones

- Todas las direcciones IP de un grupo de destino deben tener el mismo tipo de dirección IP. Por ejemplo, no puede registrar un destino IPv4 en un grupo de destino IPv6.

- Los grupos de destino de IPv6 solo se pueden usar con equilibradores de carga de `dualstack`.
- Los grupos de destino IPv6 admiten destinos de tipo IP y de instancia.

Versión del protocolo

De forma predeterminada, los equilibradores de carga de aplicaciones envían solicitudes a los destinos mediante HTTP/1.1. Puede usar la versión del protocolo para enviar solicitudes a los destinos mediante HTTP/2 o gRPC.

En la siguiente tabla se resumen el resultado de las combinaciones del protocolo de solicitud y la versión del protocolo de grupo de destino.

Protocolo de solicitud	Versión del protocolo	Resultado
HTTP/1.1	HTTP/1.1	Success
HTTP/2	HTTP/1.1	Success
gRPC	HTTP/1.1	Error
HTTP/1.1	HTTP/2	Error
HTTP/2	HTTP/2	Success
gRPC	HTTP/2	Correcto si los destinos respaldan el gRPC
HTTP/1.1	gRPC	Error
HTTP/2	gRPC	Correcto si una solicitud POST
gRPC	gRPC	Success

Consideraciones para la versión del protocolo gRPC

- El único protocolo de oyente compatible es HTTPS.
- El único tipo de acción que se admite para las reglas de oyente es `forward`.
- Solo se admiten los tipos de destino `instance` y `ip`.

- El equilibrador de carga analiza las llamadas de gRPC y las enruta a los grupos de destino adecuados en función del paquete, el servicio y el método.
- El equilibrador de carga admite la transmisión única del lado del cliente, la transmisión del lado del servidor y la transmisión bidireccional.
- Debe proporcionar un método de comprobación de estado personalizado con el formato `/package.service/method`.
- Debe especificar los códigos de estado de gRPC que deben utilizarse al comprobar si se ha recibido una respuesta correcta de un destino.
- No podrá utilizar funciones de Lambda como destinos.

Consideraciones para la versión del protocolo HTTP/2

- El único protocolo de oyente que se admite es HTTPS.
- El único tipo de acción que se admite para las reglas de oyente es `forward`.
- Solo se admiten los tipos de destino `instance` y `ip`.
- El equilibrador de carga admite la transmisión desde los clientes. El equilibrador de carga no admite la transmisión hacia los destinos.

Destinos registrados

El equilibrador de carga sirve como un único punto de contacto para los clientes y distribuye el tráfico entrante entre los destinos registrados en buen estado. Puede registrar cada destino en uno o varios grupos de destino.

Si aumenta la demanda en la aplicación, puede registrar más destinos en uno o varios grupos para controlar la demanda. El balanceador de cargas comienza a enrutar el tráfico a un destino recién registrado tan pronto como se completa el proceso de registro y el objetivo pasa la primera comprobación de estado inicial, independientemente del umbral configurado.

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

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

Límites

- No puede registrar las direcciones IP de otro Equilibrador de carga de aplicación en la misma VPC. Si el otro Equilibrador de carga de aplicación está en una VPC que está interconectada a la VPC del equilibrador de carga, puede registrar sus direcciones IP.
- No puede registrar instancias por ID de instancia si están en una VPC interconectada a la VPC del equilibrador de carga (la misma región o una región diferente). Puede registrar estas instancias por dirección IP.

Atributos del grupo de destino

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

`deregistration_delay.timeout_seconds`

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

`load_balancing.algorithm.type`

El algoritmo de equilibrador de carga determina cómo el equilibrador de carga selecciona los destinos al direccionar las solicitudes. El valor es `round_robinleast_outstanding_requests`, o`weighted_random`. El valor predeterminado es `round_robin`.

`load_balancing.algorithm.anomaly_mitigation`

Solo está disponible cuando `load_balancing.algorithm.type` está`weighted_random`. Indica si la mitigación de anomalías está habilitada. El valor es on o `off`. El valor predeterminado es `off`.

`load_balancing.cross_zone.enabled`

Indica si el equilibrio de carga entre zonas está habilitado. El valor es `true`, `false` o `use_load_balancer_configuration`. El valor predeterminado es `use_load_balancer_configuration`.

`slow_start.duration_seconds`

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

`stickiness.enabled`

Indica si están habilitadas las sesiones rápidas. El valor es `true` o `false`. El valor predeterminado es `false`.

`stickiness.app_cookie.cookie_name`

El nombre de la cookie de aplicación. El nombre de la cookie de aplicación no puede tener los siguientes prefijos: `AWSALB`, `AWSALBAPP` o`AWSALBTG`; ya que están reservados para el uso del equilibrador de carga.

`stickiness.app_cookie.duration_seconds`

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

`stickiness.lb_cookie.duration_seconds`

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

`stickiness.type`

Tipo de persistencia. Los valores posibles son `lb_cookie` y `app_cookie`.

`target_group_health.dns_failover.minimum_healthy_targets.count`

La cantidad mínima de destinos que deben estar en buen estado. Si la cantidad de destinos en buen estado es inferior a este valor, marque la zona como zona en mal estado en DNS para que el tráfico se dirija solo a las zonas que están en buen estado. Los valores posibles son `off` o un número entero comprendido entre 1 y la cantidad máxima de destinos. Cuando es `off`, la conmutación por error de DNS está deshabilitada, lo que significa que cada grupo de destino

contribuye de forma independiente a la conmutación por error de DNS. El valor predeterminado de es 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

El porcentaje mínimo de destinos que deben estar en buen estado. Si el porcentaje de destinos en buen estado es inferior a este valor, marque la zona como zona en mal estado en DNS para que el tráfico se dirija solo a las zonas que están en buen estado. Los posibles valores son `off`, o un número entero comprendido entre 1 y la cantidad máxima de destinos. Cuando es `off`, la conmutación por error de DNS está deshabilitada, lo que significa que cada grupo de destino contribuye de forma independiente a la conmutación por error de DNS. El valor predeterminado de es 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

La cantidad mínima de destinos que deben estar en buen estado. Si la cantidad de destinos en buen estado es inferior a este valor, envíe el tráfico a todos los destinos, incluidos los destinos en mal estado. El rango comprende del 1 a la cantidad máxima de destinos. El valor predeterminado de es 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

El porcentaje mínimo de destinos que deben estar en buen estado. Si el porcentaje de destinos en buen estado es inferior a este valor, envíe el tráfico a todos los destinos, incluidos los destinos en mal estado. Los valores posibles son `off` o un número entero comprendido entre 1 y 100. El valor predeterminado es `off`.

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

`lambda.multi_value_headers.enabled`

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

Los algoritmos de enrutamiento

Un algoritmo de enrutamiento es el método que utiliza el balanceador de cargas para determinar qué objetivos recibirán las solicitudes. El algoritmo de enrutamiento por turnos se utiliza de forma

predeterminada para enrutar las solicitudes a nivel del grupo objetivo. Las solicitudes menos pendientes y los algoritmos de enrutamiento aleatorio ponderado también están disponibles en función de las necesidades de su aplicación. Un grupo objetivo solo puede tener un algoritmo de enrutamiento activo a la vez, sin embargo, el algoritmo de enrutamiento se puede actualizar siempre que sea necesario.

Si habilita las sesiones permanentes, el algoritmo de enrutamiento seleccionado se utiliza para la selección inicial del destino. Las solicitudes futuras del mismo cliente se reenviarán al mismo destino, sin tener en cuenta el algoritmo de enrutamiento seleccionado.

¡Ronda contra todos!

- El algoritmo de enrutamiento por turnos enruta las solicitudes de manera uniforme entre los objetivos sanos del grupo objetivo, en orden secuencial.
- Este algoritmo se suele utilizar cuando las solicitudes que se reciben tienen una complejidad similar, los destinos registrados tienen una capacidad de procesamiento similar o si es necesario distribuir las solicitudes por igual entre los destinos.

Solicitudes menos pendientes

- El algoritmo de enrutamiento de las solicitudes menos pendientes enruta las solicitudes a los destinos con el menor número de solicitudes en curso.
- Este algoritmo se suele utilizar cuando las solicitudes que se reciben varían en complejidad y los objetivos registrados varían en cuanto a su capacidad de procesamiento.
- Cuando un balanceador de cargas compatible con HTTP/2 utiliza destinos que solo admiten HTTP/1.1, convierte la solicitud en varias solicitudes HTTP/1.1. En esta configuración, el algoritmo de solicitudes menos pendientes tratará cada solicitud de HTTP/2 como solicitudes múltiples.
- Cuando se utiliza WebSockets, el objetivo se selecciona mediante el algoritmo de solicitudes menos pendientes. Una vez seleccionado, el balanceador de carga crea una conexión con el destino y envía todos los mensajes a través de esta conexión.
- El algoritmo de enrutamiento de solicitudes menos pendientes no se puede utilizar con el modo de inicio lento.

Ponderado al azar

- El algoritmo de enrutamiento aleatorio ponderado enruta las solicitudes de manera uniforme entre los objetivos sanos del grupo objetivo, en orden aleatorio.

- Este algoritmo admite la mitigación de anomalías de los pesos objetivo automáticos (ATW).
- El algoritmo de enrutamiento aleatorio ponderado no se puede utilizar con el modo de inicio lento.

Modifique el algoritmo de enrutamiento de un grupo objetivo

Puede modificar el algoritmo de enrutamiento de su grupo objetivo en cualquier momento.

Para modificar el algoritmo de enrutamiento mediante la nueva consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la página de detalles de los grupos objetivo, en la pestaña Atributos, seleccione Editar.
5. En la página Editar los atributos del grupo objetivo, en la sección Configuración del tráfico, en Algoritmo de equilibrio de carga, selecciona Por turnos, Solicitudes menos pendientes o Ponderadas de forma aleatoria.
6. Elija Guardar cambios.

Para modificar el algoritmo de enrutamiento mediante AWS CLI

Utilice el comando modify-target-group-attributes con el atributo `load_balancing.algorithm.type`.

Pesos objetivo automáticos (ATW)

Los pesos objetivo automáticos (ATW) supervisan constantemente los objetivos en los que se ejecutan sus aplicaciones y detectan desviaciones de rendimiento significativas, conocidas como anomalías. El ATW permite ajustar dinámicamente la cantidad de tráfico que se dirige a los objetivos mediante la detección de anomalías en los datos en tiempo real.

Automatic Target Weights (ATW) detecta automáticamente las anomalías en todos los Application Load Balancer de tu cuenta. Cuando se identifican objetivos anómalos, ATW puede intentar estabilizarlos automáticamente reduciendo la cantidad de tráfico a los que se enrutan, lo que se conoce como mitigación de anomalías. ATW optimiza continuamente la distribución del tráfico para

maximizar las tasas de éxito por objetivo y, al mismo tiempo, minimizar las tasas de fracaso del grupo objetivo.

Consideraciones:

- En la actualidad, la detección de anomalías monitorea los códigos de respuesta HTTP 5xx que provienen de sus objetivos y los fallos de conexión con ellos. La detección de anomalías está siempre activada y no se puede desactivar.
- No se admite ATW cuando se utiliza Lambda como objetivo.

Detección de anomalías

La detección de anomalías ATW monitorea cualquier objetivo que muestre una desviación significativa en su comportamiento con respecto a otros objetivos de su grupo objetivo. Estas desviaciones, denominadas anomalías, se determinan comparando el porcentaje de errores de un objetivo con el porcentaje de errores de otros objetivos del grupo objetivo. Estos errores pueden ser tanto errores de conexión como códigos de error HTTP. Los objetivos que reportan cifras significativamente más altas que sus pares se consideran anómalos.

La detección de anomalías requiere un mínimo de tres objetivos sanos en el grupo objetivo. Cuando un objetivo está registrado en un grupo objetivo, primero tiene que pasar los controles de estado para empezar a recibir tráfico. Una vez que el objetivo recibe el objetivo, ATW comienza a monitorizarlo y publica continuamente el resultado de la anomalía. En el caso de los objetivos sin anomalías, el resultado de la anomalía es. `normal` En el caso de los objetivos con anomalías, el resultado de la anomalía es. `anomalous`

La detección de anomalías ATW funciona independientemente de los controles de estado del grupo objetivo. Un objetivo puede superar todos los controles de estado del grupo objetivo, pero aun así ser marcado como anómalo debido a una elevada tasa de error. El hecho de que los objetivos pasen a ser anómalos no afecta al estado de las comprobaciones de estado del grupo objetivo.

Estado de detección de anomalías

ATW publica continuamente el estado de las detecciones de anomalías que realiza en los objetivos. Puede ver el estado actual en cualquier momento utilizando la tecla o. AWS Management Console AWS CLI

Para ver el estado de detección de anomalías mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la página de detalles de los grupos objetivo, seleccione la pestaña Objetivos.
5. En la tabla de objetivos registrados, puede ver el estado de las anomalías de cada objetivo en la columna de resultados de la detección de anomalías.

   Si no se detectó ninguna anomalía, el resultado es. `normal`

   Si se detectaron anomalías, el resultado es. `anomalous`

Para ver los resultados de la detección de anomalías mediante el AWS CLI

Utilice el comando describe-target-health con el valor del atributo establecido en. `Include.member.N` `AnomalyDetection`

Mitigación de anomalías

> **Important**
>
> La función de mitigación de anomalías de ATW solo está disponible cuando se utiliza el algoritmo de enrutamiento aleatorio ponderado.

La mitigación de anomalías ATW desvía automáticamente el tráfico de los objetivos anómalos, lo que les da la oportunidad de recuperarse.

Durante la mitigación:

- La ATW ajusta periódicamente la cantidad de tráfico que se dirige a objetivos anómalos. Actualmente, el período es cada cinco segundos.
- El ATW reduce la cantidad de tráfico que se dirige a objetivos anómalos al mínimo necesario para mitigar las anomalías.
- A los objetivos que ya no se detecten como anómalos se les dirigirá gradualmente más tráfico hasta que alcancen la paridad con otros objetivos normales del grupo objetivo.

Activa la mitigación de anomalías ATW

Puedes activar la mitigación de anomalías en cualquier momento.

Para activar la mitigación de anomalías mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la página de detalles de los grupos objetivo, en la pestaña Atributos, selecciona Editar.
5. En la página Editar los atributos del grupo objetivo, en la sección Configuración del tráfico, en Algoritmo de equilibrio de carga, asegúrese de seleccionar Ponderado aleatorio.

   Nota: Cuando se selecciona inicialmente el algoritmo aleatorio ponderado, la detección de anomalías está activada de forma predeterminada.
6. En Mitigación de anomalías, asegúrate de que esté seleccionada la opción Activar la mitigación de anomalías.
7. Elija Guardar cambios.

Para activar la mitigación de anomalías mediante la AWS CLI

Utilice el comando modify-target-group-attributes con el atributo `load_balancing.algorithm.anomaly_mitigation`.

Estado de mitigación de anomalías

Siempre que ATW lleve a cabo una mitigación en un objetivo, podrá ver el estado actual en cualquier momento utilizando la AWS Management Console tecla o. AWS CLI

Para ver el estado de la mitigación de anomalías mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la página de detalles de los grupos objetivo, seleccione la pestaña Objetivos.

5. En la tabla de objetivos registrados, puedes ver el estado de mitigación de las anomalías de cada objetivo en la columna Mitigación en vigor.

   Si la mitigación no está en curso, el estado es`yes`.

   Si la mitigación está en curso, el estado es`no`.

Para ver el estado de mitigación de anomalías mediante el AWS CLI

Utilice el comando describe-target-health con el valor del atributo establecido en. `Include.member.N` `AnomalyDetection`

Retardo de anulación del registro

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

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

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

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

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

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

2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Editar atributos, cambie el valor de Retardo de anulación de registro según sea necesario.
6. Elija Guardar cambios.

Para actualizar el valor del retraso en la cancelación del registro mediante el AWS CLI

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

Modo de inicio lento

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

Después de habilitar el inicio lento para un grupo de destino, sus destinos entran en modo de inicio lento cuando el grupo de destino los considera en buen estado. Un destino en modo de inicio lento sale de este modo cuando transcurre el período de duración de inicio lento configurado o el destino deja de estar en buen estado. El equilibrador de carga aumenta linealmente el número de solicitudes que puede enviar a un destino en modo de inicio lento. Una vez que un destino en buen estado sale del modo de inicio lento, el equilibrador de carga puede enviarle una cuota completa de solicitudes.

Consideraciones

- Al habilitar el inicio lento para un grupo de destino, los destinos en buen estado registrados en el grupo de destino no entran en el modo de inicio lento.
- Al habilitar el inicio lento para un grupo de destino vacío y, a continuación, registrar varios destinos mediante una operación de registro único, estos destinos no entran en el modo de inicio lento. Los destinos recién registrados entran en el modo de inicio lento solo cuando hay al menos un destino en buen estado que no está en modo de inicio lento.

- Si anula el registro de un destino en modo de inicio lento, el destino sale del modo de inicio lento. Si vuelve a registrar el mismo destino, este entra en modo de inicio lento cuando el grupo de destino lo considere en buen estado.
- Si un destino en modo de inicio lento dejar de estar en buen estado, el destino sale del modo de inicio lento. Cuando el destino está en buen estado, este vuelve a entrar en el modo de inicio lento.
- No se puede activar el modo de inicio lento cuando se utilizan las solicitudes menos pendientes o los algoritmos de enrutamiento aleatorio ponderado.

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

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Editar atributos, cambie el valor de Duración de inicio lento según sea necesario y, a continuación, seleccione Guardar. Para deshabilitar el modo de inicio lento, establezca la duración en 0.
6. Elija Guardar cambios.

Para actualizar el valor de duración del inicio lento mediante el AWS CLI

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

Crear un grupo de destino.

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

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

Para direccionar el tráfico a los destinos de un grupo de destino, especifique el grupo de destino en una acción al crear un oyente o crear una regla para este último. Para obtener más información, consulte Reglas del oyente. Puede especificar el mismo grupo de destino en varios oyentes, pero estos oyentes deben pertenecer al mismo Equilibrador de carga de aplicación. Para usar un grupo

de destino con un equilibrador de carga, debe comprobar que el grupo de destino no esté siendo utilizado por un oyente para ningún otro equilibrador de carga.

Puede agregar o eliminar destinos del grupo de destino en cualquier momento. Para obtener más información, consulte Registro de destinos con el grupo de destino. También puede modificar la configuración de la comprobación de estado del grupo de destino. Para obtener más información, consulte Modificar la configuración de comprobación de estado de un grupo de destino.

Para crear un grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija Crear grupo de destino.
4. En Tipo de destino, seleccione Instancia para registrar los destinos por ID de instancia, IP para registrar direcciones IP y función de Lambda para registrar una función de Lambda.
5. En Target group name, escriba el nombre del nuevo grupo de destino. Este nombre debe ser único por región por cuenta, puede tener un máximo de 32 caracteres, debe contener únicamente caracteres alfanuméricos o guiones y no puede comenzar ni terminar con un guion.
6. (Opcional) En Protocol y Port, modifique los valores predeterminados según sea necesario.
7. Si el tipo de destino es Instancias o direcciones IP, elija IPv4 o IPv6 como tipo de dirección IP; de lo contrario, pase al siguiente paso.

   Tenga en cuenta que solo los destinos con el tipo de dirección IP seleccionado se pueden incluir en este grupo de destinos. Una vez creado el grupo de destino, el tipo de dirección IP ya no se podrá modificar.
8. En VPC, seleccione una nube privada virtual (VPC). Tenga en cuenta que para tipos de destino de direcciones IP, las VPC disponibles para su selección son aquellas que admiten el tipo de dirección IP que eligió en el paso anterior.
9. (Opcional) En Versión del protocolo, modifique los valores predeterminados según sea necesario.
10. (Opcional) En la sección Comprobaciones de estado, mantenga la configuración predeterminada.
11. Si el tipo de destino es la función de Lambda, puede habilitar las comprobaciones de estado seleccionando Habilitar en la sección Comprobaciones de estado.
12. (Opcional) Agregue una o varias etiquetas, como se indica a continuación:

a. Expanda la sección Etiquetas.
b. Seleccione Agregar etiqueta.
c. Escriba la clave y el valor de la etiqueta.

13. Elija Siguiente.
14. (Opcional) Agregue uno o varios destinos, como se indica a continuación:
    - Si el tipo de destino es Instancias, seleccione una o más instancias, introduzca uno o más puertos y, a continuación, elija Incluir como pendiente debajo.

      Nota: Las instancias deben tener una dirección IPv6 principal asignada para poder registrarse en un grupo de destino de IPv6.
    - Si el tipo de destino es direcciones IP, haga lo siguiente:

      a. Seleccione una VPC de red de la lista o elija Otras direcciones IP privadas.
      b. Introduzca la dirección IP manualmente o busque la dirección IP mediante los detalles de la instancia. Puede introducir hasta cinco direcciones IP a la vez.
      c. Introduzca los puertos para enrutar el tráfico a las direcciones IP especificadas.
      d. Seleccione Incluir como pendiente debajo.
    - Si el tipo de destino es una función de Lambda, especifique una sola u omita este paso y especifique una función de Lambda más adelante.
15. Elija Crear grupo de destino.
16. (Opcional) Puede especificar el grupo de destino en una regla de oyente. Para obtener más información, vea Reglas del oyente.

Para crear un grupo objetivo mediante el AWS CLI

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

Comprobaciones de estado de los grupos de destino

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

Cada nodo del equilibrador de carga direcciona las solicitudes únicamente a los destinos en buen estado de las zonas de disponibilidad habilitadas para el equilibrador de carga. Cada nodo del

equilibrador de carga comprueba el estado de cada destino; para ello, utiliza la configuración de comprobación de estado de los grupos de destino en los que está registrado el destino. Una vez que el destino está registrado, debe superar una comprobación de estado para que se considere que se encuentra en buen estado. Después de completar cada comprobación de estado, el nodo del equilibrador de carga cierra la conexión se estableció para la comprobación de estado.

Si un grupo de destino contiene solo destinos registrados en mal estado, el equilibrador de carga dirige las solicitudes a todos esos destinos, independientemente de su estado. Esto significa que si todos los destinos no pasan las comprobaciones de estado al mismo tiempo en todas las zonas de disponibilidad habilitadas, el equilibrador de carga no se abrirá correctamente. El efecto de la apertura por error es permitir que el tráfico llegue a todos los destinos de todas las zonas de disponibilidad habilitadas, independientemente de su estado, en función del algoritmo de equilibrio de carga.

Los controles de salud no son compatibles WebSockets.

Configuración de comprobación de estado

Puede configurar las comprobaciones de estado de los destinos de un grupo de destino según se indica en la siguiente tabla. Los nombres de configuración que se utilizan en la tabla son los que se utilizan en la API. El balanceador de cargas envía una solicitud de comprobación de estado a cada objetivo registrado cada HealthCheckIntervalSecondssegundo, mediante el puerto, el protocolo y la ruta de comprobación de estado especificados. Cada solicitud de comprobación de estado es independiente y el resultado dura todo el intervalo. El tiempo que tarda el destino en responder no afecta al intervalo de la siguiente solicitud de comprobación de estado. Si las comprobaciones de estado superan los errores UnhealthyThresholdCountconsecutivos, el equilibrador de cargas deja el objetivo fuera de servicio. Cuando las comprobaciones de estado superan las HealthyThresholdCountcorrectas consecutivas, el equilibrador de cargas vuelve a poner el objetivo en servicio.

Opción	Descripción
HealthCheckProtocol	Protocolo que el equilibrador de carga utiliza al realizar comprobaciones de estado en los destinos. Los posibles protocolos son HTTP y HTTPS. El valor predeterminado es el protocolo HTTP.

Opción	Descripción
	Estos protocolos utilizan el método HTTP GET para enviar las solicitudes de comprobación de estado.
HealthCheckPort	Puerto que el equilibrador de carga utiliza al realizar comprobaciones de estado en los destinos. El valor predeterminado es el puerto en el que cada destino recibe el tráfico procedente del equilibrador de carga.
HealthCheckPath	El destino para las comprobaciones de estado en los destinos. Si la versión del protocolo es HTTP/1.1 o HTTP/2, especifique un URI válido (/ruta?consulta). El valor predeterminado es /. Si la versión del protocolo es gRPC, especifiq ue la ruta del método de comprobación de estado personalizado con el formato `/package.service/method` . El valor predeterminado es `/AWS.ALB/healthche ck` .
HealthCheckTimeoutSeconds	Cantidad de tiempo, en segundos, durante la cual ninguna respuesta de un destino significa una comprobación de estado fallida. El rango va de 2 a 120 segundos. El valor predeterm inado es 5 segundos si el tipo de destino es `instance` o `ip` y 30 segundos si el tipo de destino es `lambda`.

Opción	Descripción
HealthCheckIntervalSeconds	Cantidad aproximada de tiempo, en segundos, que transcurre entre comprobaciones de estado de un destino individual. El rango va de 5 a 300 segundos. El valor predeterminado es 30 segundos si el tipo de destino es `instance` o `ip` y 35 segundos si el tipo de destino es `lambda`.
HealthyThresholdCount	Número de comprobaciones de estado consecutivas que deben superarse para considerar que un destino en mal estado vuelve a estar en buen estado. El rango va de 2 a 10. El valor predeterminado es 5.
UnhealthyThresholdCount	Número de comprobaciones de estado consecutivas no superadas que se requieren para considerar que un destino se encuentra en mal estado. El rango va de 2 a 10. El valor predeterminado es 2.

Opción	Descripción
Matcher	Códigos que se deben utilizar al comprobar si se ha recibido una respuesta exitosa de un destino. En la consola, se denominan códigos de éxito. Si la versión del protocolo es HTTP/1.1 o HTTP/2, los valores posibles oscilan entre 200 y 499. Puede especificar varios valores (por ejemplo, “200,202”) o un intervalo de valores (por ejemplo, “200-299”). El valor predeterm inado es 200. Si la versión del protocolo es gRPC, los valores posibles van de 0 a 99. Puede especific ar varios valores (por ejemplo, “0,1”) o un intervalo de valores (por ejemplo, “0-5”). El valor predeterminado es 12.

Estado del destino

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

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

Valor	Descripción
`initial`	El equilibrador de carga se encuentra en proceso de registrar el destino o de realizar las comprobaciones de estado iniciales en el destino.

Valor	Descripción
	Códigos de motivo relacionados: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	El destino se encuentra en buen estado. Códigos de motivo relacionados: ninguno
`unhealthy`	El destino no respondió a una comprobación de estado o no la ha superado. Códigos de motivo relacionados: `Target.ResponseCodeMismatch` | `Target.Timeout` | `Target.FailedHealthChecks` | `Elb.InternalError`
`unused`	El destino no está registrado en un grupo de destino, el grupo de destino no se utiliza en una regla del oyente, el destino se encuentra en una zona de disponibilidad que no está habilitada o el destino está en un estado detenido o terminado. Códigos de motivo relacionados: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`
`draining`	El destino está en proceso de anulación del registro y de vaciado de conexiones. Código de motivo relacionado: `Target.DeregistrationInProgress`
`unavailable`	Las comprobaciones de estado están deshabilitadas para el grupo de destino. Código de motivo relacionado: `Target.HealthCheckDisabled`

Códigos de motivo de comprobación de estado

Si el estado de un destino es un valor distinto de `Healthy`, el API devuelve un código de motivo y una descripción del problema, y la consola muestra la misma descripción. Los códigos de motivo que comienzan por `Elb` tienen su origen en el equilibrador de carga y que los códigos de motivo que comienzan por `Target` tienen su origen en el destino. Para obtener más información sobre las posibles causas de los errores en las comprobaciones de estado, consulte Solución de problemas.

Código de motivo	Descripción
`Elb.InitialHealthChecking`	Las comprobaciones de estado iniciales están en curso.
`Elb.InternalError`	Las comprobaciones de estado no se han superado debido a un error interno.
`Elb.RegistrationInProgress`	El registro del destino está en curso.
`Target.DeregistrationInProgress`	La anulación del registro del destino está en curso.
`Target.FailedHealthChecks`	Las comprobaciones de estado no se han superado.
`Target.HealthCheckDisabled`	Las comprobaciones de estado están deshabilitadas
`Target.InvalidState`	El destino se encuentra en estado detenido. El destino se encuentra en estado terminado. El destino se encuentra en estado terminado o detenido. El destino se encuentra en un estado no válido.
`Target.IpUnusable`	La dirección IP no se puede utilizar como destino, ya que la utiliza un equilibrador de carga.
`Target.NotInUse`	El grupo de destino no se ha configurado para recibir el tráfico del equilibrador de carga.

Código de motivo	Descripción
	El destino se encuentra en una zona de disponibilidad que no está habilitada para el equilibrador de carga.
`Target.NotRegistered`	El destino no está registrado en el grupo de destino.
`Target.ResponseCodeMismatch`	Las comprobaciones de estado no se han superado y se han emitido estos códigos: [código]
`Target.Timeout`	Se agotó el tiempo de espera de la solicitud.

Comprobación del estado de los destinos

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

Para comprobar el estado de los destinos desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Seleccione el nombre del grupo de destino para abrir la página de detalles.
4. En la pestaña Targets la Status columna indica el estado de cada destino.
5. Si el estado es un valor distinto de `Healthy`, la columna Detalles del estado contiene más información. Para obtener ayuda con los errores en las comprobaciones de estado, consulte Solución de problemas.

Para comprobar el estado de tus objetivos, utiliza el AWS CLI

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

Para recibir notificaciones por correo electrónico sobre destinos en mal estado

Utilice CloudWatch alarmas para activar una función Lambda que envíe detalles sobre objetivos en mal estado. Para step-by-step obtener instrucciones, consulta la siguiente entrada del blog: Cómo identificar los objetivos insalubres de tu balanceador de cargas.

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

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

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

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Configuración de comprobación de estado, seleccione Editar.
5. En la página Editar la configuración de la comprobación de estado, modifique la configuración según sea necesario y, a continuación, seleccione Guardar cambios.

Para modificar la configuración de las comprobaciones de estado de un grupo objetivo mediante el AWS CLI

Utilice el comando modify-target-group.

Equilibrio de carga entre zonas para grupos de destino

Los nodos del equilibrador de carga distribuyen las solicitudes procedentes de los clientes entre los destinos registrados. Cuando el equilibrio de carga entre zonas está habilitado, cada nodo del equilibrador de carga distribuye el tráfico entre los destinos registrados de todas las zonas de disponibilidad habilitadas. Cuando el equilibrio de carga entre zonas está deshabilitado, cada nodo del equilibrador de carga distribuye el tráfico únicamente entre los destinos registrados de su zona de disponibilidad. Esto puede ser si se prefieren los dominios de fallos zonales en lugar de los regionales, para garantizar que una zona en buen estado no se vea afectada por una zona en mal estado o para mejorar la latencia general.

Con los equilibradores de carga de aplicaciones, el equilibrio de carga entre zonas siempre está activado en el nivel del equilibrador de carga y no se puede desactivar. Para los grupos de destino, la configuración del equilibrador de carga está predeterminada, pero puede anularla activando o desactivando explícitamente el equilibrio de carga entre zonas al nivel del grupo de destino.

Consideraciones

- La pertinencia de destino no está adminitda cuando equilibrio de carga entre zonas está deshabilitado.
- Las funciones de Lambda como destinos no son admitidos cuando un equilibrador de carga entre zonas está deshabilitado.
- Si se intenta desactivar el equilibrio de carga entre zonas a través de la API de `ModifyTargetGroupAttributes`, si los destinos tienen `AvailabilityZone` de parámetros establecidos en resultados de `all` en un error.
- Al registrar los destinos, el parámetro de `AvailabilityZone` es obligatorio. Después de crear un equilibrador de carga entre zonas en cualquier momento, el equilibrio de carga entre zonas está deshabilitado. De lo contrario, el parámetro se ignora y se trata como `all`.

Prácticas recomendadas

- Planifique una capacidad de destino suficiente en todas las zonas de disponibilidad que prevé utilizar, por grupo de destino. Si no puede planificar una capacidad suficiente en todas las zonas de disponibilidad participantes, recomendamos que mantenga activado el equilibrio de carga entre zonas.
- Al configurar su equilibrador de carga de aplicación con varios grupos de destino, asegúrese de que todos los grupos de destino participen en las mismas zonas de disponibilidad, dentro de la región configurada. Esto evita que una zona de disponibilidad quede vacía mientras el equilibrio de carga entre zonas esté desactivado, ya que provoca un error 503 en todas las solicitudes HTTP que entran en la zona de disponibilidad vacía.
- Evite crear subredes vacías. Los equilibradores de carga de aplicaciones exponen las direcciones IP de zona a través del DNS para las subredes vacías, lo que desencadena errores 503 en las solicitudes HTTP.
- En algunos casos, un grupo de destino con el equilibrio de carga entre zonas desactivado tiene una capacidad de destino planificada suficiente por zona de disponibilidad, pero todos los destinos de una zona de disponibilidad dejan de funcionar correctamente. Cuando hay al menos un grupo de destino con todos los destinos en un estado, las direcciones IP de los nodos del equilibrador de carga se eliminan del DNS. Cuando el grupo de destino tiene al menos un destino en buen estado, las direcciones IP se restauran en el DNS.

Deshabilitar el equilibrio de carga entre zonas

Puede deshabilitar un equilibrador de carga entre zonas para sus grupos de destino del equilibrador de carga de aplicación en cualquier momento.

Para deshabilitar el equilibrio de carga entre zonas desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el nombre del grupo de destino para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar los atributos del grupo de destino, seleccione Deshabilitar para el equilibrio de carga entre zonas.
6. Elija Save changes (Guardar cambios).

Para deshabilitar el equilibrio de carga entre zonas desde la AWS CLI

Utilice el comando modify-target-group-attributes y establezca el atributo `load_balancing.cross_zone.enabled` en `false`.

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=false
```

A continuación, se muestra un ejemplo de respuesta:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "false"
        },
    ]
}
```

Habilitar equilibrio de carga entre zonas

Puede habilitar un equilibrador de carga entre zonas para sus grupos de destino del equilibrador de carga de aplicación en cualquier momento. La configuración del equilibrio de carga entre zonas a nivel del grupo de destino anula la configuración a nivel del equilibrador de carga.

Para habilitar el equilibrio de carga entre zonas desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el nombre del grupo de destino para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar los atributos del grupo de destino, seleccione Habilitar para el equilibrio de carga entre zonas.
6. Elija Save changes (Guardar cambios).

Para habilitar el equilibrio de carga entre zonas desde la AWS CLI

Utilice el comando modify-target-group-attributes y establezca el atributo `load_balancing.cross_zone.enabled` en `true`.

```
aws elbv2 modify-target-group-attributes --target-group-arn my-targetgroup-arn --
attributes Key=load_balancing.cross_zone.enabled,Value=true
```

A continuación, se muestra un ejemplo de respuesta:

```
{
    "Attributes": [
        {
            "Key": "load_balancing.cross_zone.enabled",
            "Value": "true"
        },
    ]
}
```

Estado del grupo de destino

De forma predeterminada, un grupo de destino se considera en buen estado siempre que tenga al menos un destino en buen estado. Si tiene una flota grande, no basta con tener un solo destino en buen estado que atienda el tráfico. En su lugar, puede especificar un recuento o porcentaje mínimo de destinos que deben estar en buen estado y qué acciones tomará el equilibrador de carga cuando los destinos en buen estado estén por debajo del umbral especificado. Esto puede mejorar la disponibilidad.

Acciones en mal estado

Puede configurar umbrales de buen estado para las siguientes acciones:

- Conmutación por error de DNS: cuando los destinos en buen estado de una zona están por debajo del umbral, marcamos las direcciones IP del nodo del equilibrador de carga de la zona como en mal estado en el DNS. Por lo tanto, cuando los clientes resuelven el nombre DNS del equilibrador de carga, el tráfico se enruta únicamente a las zonas en buen estado.
- Conmutación por error de enrutamiento: cuando los destinos en buen estado de una zona están por debajo del umbral, el equilibrador de carga envía tráfico a todos los destinos que están disponibles para el nodo del equilibrador de carga, incluidos los destinos en mal estado. Esto aumenta las probabilidades de que la conexión de un cliente se realice correctamente, en particular cuando los destinos no pasan temporalmente las comprobaciones de estado, y reduce el riesgo de sobrecargar los destinos en buen estado.

Requisitos y consideraciones

- Esta característica no se puede utilizar con grupos de destino en los que el destino es una función de Lambda. Si el Equilibrador de carga de aplicación es el destino de un Equilibrador de carga de red o Global Accelerator, no configure un umbral para la conmutación por error de DNS.
- Si especifica ambos tipos de umbrales para una acción (recuento y porcentaje), el equilibrador de carga realizará la acción cuando se supere alguno de los umbrales.
- Si especifica umbrales para ambas acciones, el umbral de la conmutación por error de DNS debe ser mayor o igual que el umbral de la conmutación por error de enrutamiento, de modo que la conmutación por error de DNS se produzca al mismo tiempo que la conmutación por error de enrutamiento o antes.

- Si especifica el umbral como un porcentaje, calculamos el valor de forma dinámica en función de la cantidad total de destinos registrados en los grupos de destino.
- La cantidad total de destinos se basa en si el equilibrio de carga entre zonas está activado o desactivado. Si el equilibrio de carga entre zonas está desactivado, cada nodo envía tráfico solo a los destinos de su propia zona, lo que significa que los umbrales se aplican a la cantidad de destinos de cada zona habilitada por separado. Si el equilibrio de carga entre zonas está activado, cada nodo envía tráfico a todos los destinos de todas las zonas habilitadas, lo que significa que los umbrales especificados se aplican a la cantidad total de destinos de todas las zonas habilitadas.
- Con la conmutación por error de DNS, eliminamos las direcciones IP de las zonas en mal estado del nombre de host DNS del equilibrador de carga. Sin embargo, la caché de DNS del cliente local puede contener estas direcciones IP hasta que caduque el time-to-live (TTL) del registro DNS (60 segundos).
- Cuando se produce una conmutación por error de DNS, esto afecta todos los grupos de destino asociados al equilibrador de carga. Asegúrese de tener suficiente capacidad en las zonas restantes para gestionar este tráfico adicional, especialmente si el equilibrio de carga entre zonas está desactivado.
- Con la conmutación por error de DNS, si se considera que todas las zonas del equilibrador de carga están en mal estado, el equilibrador de carga envía tráfico a todas las zonas, incluidas las zonas en mal estado.
- Existen otros factores, además de la existencia de suficientes destinos en buen estado, que podrían provocar una conmutación por error de DNS, como el estado de la zona.

Supervisión

Para supervisar el estado de los grupos objetivo, consulte CloudWatch las métricas del estado de los grupos objetivo.

Ejemplo

En el siguiente ejemplo, se muestra cómo se aplica la configuración de estado del grupo de destino.

Escenario

- Un equilibrador de carga que admite dos zonas de disponibilidad, A y B
- Cada zona de disponibilidad contiene 10 destinos registrados
- El grupo de destino tiene la siguiente configuración de estado del grupo de destino:

  - Conmutación por error de DNS: 50 %
  - Conmutación por error de enrutamiento: 50 %
- Seis destinos fallan en la zona de disponibilidad B

Cuando el equilibrio de carga entre zonas está desactivado

- El nodo del equilibrador de carga de cada zona de disponibilidad solo puede enviar tráfico a los 10 destinos de su zona de disponibilidad.
- Hay 10 destinos en buen estado en la zona de disponibilidad A que cumplen con el porcentaje requerido de destinos en buen estado. El equilibrador de carga sigue distribuyendo el tráfico entre los 10 destinos en buen estado.
- Solo hay 4 destinos en buen estado en la zona de disponibilidad B, es decir, el 40% de los destinos del nodo del equilibrador de carga de la zona de disponibilidad B. Como este porcentaje es inferior al porcentaje de destinos en buen estado requerido, el equilibrador de carga toma las siguientes medidas:
  - Conmutación por error de DNS: la zona de disponibilidad B está marcada como en mal estado en el DNS. Como los clientes no pueden resolver el nombre del equilibrador de carga en el nodo del equilibrador de carga de la zona de disponibilidad B y la zona de disponibilidad A está en buen estado, los clientes envían nuevas conexiones a la zona de disponibilidad A.
  - Conmutación por error de enrutamiento: cuando se envían nuevas conexiones de forma explícita a la zona de disponibilidad B, el equilibrador de carga distribuye el tráfico a todos los destinos de la zona de disponibilidad B, incluidos los destinos en mal estado. Esto evita interrupciones entre los demás destinos en buen estado.

Cuando el equilibrio de carga entre zonas está activado

- Cada nodo del equilibrador de carga puede enviar tráfico a los 20 destinos registrados en ambas zonas de disponibilidad.
- Hay 10 destinos en buen estado en la zona de disponibilidad A y 4 destinos en buen estado en la zona de disponibilidad B, con un total de 14 destinos en buen estado. Esto representa el 70% de los destinos de los nodos del equilibrador de carga en ambas zonas de disponibilidad, lo que cumple con el porcentaje requerido de destinos en buen estado.
- El equilibrador de carga distribuye el tráfico entre los 14 destinos en buen estado en ambas zonas de disponibilidad.

Modificación de la configuración de estado de grupo de destino

Puede modificar la configuración del estado de grupo de destino de su grupo de destino de la siguiente manera.

Para modificar la configuración del estado de grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Compruebe si el equilibrio de carga entre zonas está activado o desactivado. Actualice esta configuración según sea necesario para asegurarse de que tiene suficiente capacidad para gestionar el tráfico adicional en caso de que falle una zona.
6. Amplíe los requisitos de estado del grupo de destino.
7. Para el tipo de configuración, le recomendamos que elija la configuración unificada, que establece el mismo umbral para ambas acciones.
8. Para conocer los requisitos para un buen estado, realice una de las siguientes acciones:
   - Elija Recuento mínimo de destinos en buen estado y, a continuación, introduzca un número entre 1 y el número máximo de destinos para su grupo de destino.
   - Elija el porcentaje mínimo de destinos en buen estado y, a continuación, introduzca un número del 1 al 100.
9. Elija Guardar cambios.

Para modificar la configuración de salud del grupo objetivo mediante el AWS CLI

Utilice el comando modify-target-group-attributes. En el siguiente ejemplo, se establece el umbral de buen estado para ambas acciones de mal estado en un 50 %.

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-targets/73e2d6bc24d8a067 \
--attributes
 Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \

 Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

Uso de la conmutación por error de DNS de Route 53 para el equilibrador de carga

Si utiliza Route 53 para dirigir las consultas de DNS al equilibrador de carga, también puede utilizar Route 53 para configurar la conmutación por error de DNS del equilibrador de carga. En una configuración de conmutación por error, Route 53 comprueba el estado de los destinos del grupo de destino para el equilibrador de carga con el fin de determinar si están disponibles. Si no existen destinos en buen estado registrados en el equilibrador de carga o si este no se encuentra en buen estado, Route 53 enruta el tráfico a otro recurso disponible, como un equilibrador de carga en buen estado o un sitio web estático en Amazon S3.

Por ejemplo, supongamos que tenemos una aplicación web para `www.example.com` y deseamos ejecutar instancias redundantes por detrás de dos equilibradores de carga que residen en regiones distintas. Queremos enrutar el tráfico principalmente al equilibrador de carga de una de las regiones y utilizar el equilibrador de carga de la otra región como copia de seguridad en caso de error. Si configura la conmutación por error de DNS, puede especificar los equilibradores de carga principal y secundario (de copia de seguridad). Route 53 enruta el tráfico al equilibrador de carga principal si está disponible, o bien, en caso contrario, al secundario.

Uso de Evaluate Target Health

- Cuando Evaluate Target Health se establece en `Yes` en un registro de alias para un Equilibrador de carga de aplicación, Route 53 evalúa el estado del recurso especificado por el valor de `alias target`. Para un Equilibrador de carga de aplicación, Route 53 utiliza las comprobaciones de estado del grupo de destino asociadas al equilibrador de carga.
- Cuando todos los grupos de destino de un Equilibrador de carga de aplicación están en buen estado, Route 53 marca el registro del alias como en buen estado. Si un grupo de destino contiene al menos un destino en buen estado, se aprueba la comprobación de estado del grupo de destino. 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.
- Si alguno de los grupos de destino de un Equilibrador de carga de aplicación está en mal estado, el registro de alias no pasa la comprobación de estado de Route 53 (apertura por error). Si se utiliza la evaluación del estado del destino, no se aplicará la política de enrutamiento de conmutación por error.
- Si todos los grupos de destino de un Equilibrador de carga de aplicación están vacíos (no hay destinos), Route 53 considera que el registro está en mal estado (apertura por error). Si se utiliza

la evaluación del estado del destino, no se aplicará la política de enrutamiento de conmutación por error.

Para obtener más información, consulte Configuración de la conmutación por error de DNS en la Guía para desarrolladores de Amazon Route 53.

Registro de destinos con el grupo de destino

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

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

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

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

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

Si está registrando destinos por ID de instancia, puede utilizar el equilibrador de carga con un grupo de escalado automático. Después de asociar un grupo de destino a un grupo de escalado automático y cuando el grupo escala horizontalmente, las instancias lanzadas por el grupo de escalado automático se registran automáticamente en el grupo de destino. Si separa el grupo de destino del grupo de escalado automático, automáticamente se anula el registro de las instancias en el grupo de destino. Para obtener más información, consulte Adjuntar un equilibrador de carga al grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.

Grupos de seguridad de destino

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

Reglas recomendadas

Inbound

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

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

Subredes compartidas

Los participantes pueden crear un Equilibrador de carga de aplicación en una VPC compartida. Los participantes no pueden registrar un destino que se ejecute en una subred que no esté compartida con ellos.

Registro o anulación del registro de destinos

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

Contenido

- Registro o anulación del registro de destinos por ID de instancia
- Registro o anulación del registro de destinos por dirección IP

- Registrar o anular el registro de una función de Lambda
- Registro o anulación del registro de destinos mediante la AWS CLI

Registro o anulación del registro de destinos por ID de instancia

> **Note**
>
> Al registrar los destinos por ID de instancia para un grupo de destinos IPv6, los destinos deben tener una dirección IPv6 principal asignada. Para obtener más información, consulte las direcciones IPv6 en la Guía del usuario de Amazon EC2

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

Para registrar un destino o anular su registro mediante el ID de instancia desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Para registrar instancias, elija Registrar destinos. Seleccione una o más instancias, ingrese el puerto de instancia predeterminado según sea necesario y, a continuación, elija Incluir como pendiente debajo. Cuando haya terminado de agregar instancias, elija Registrar destinos pendientes.

   Nota:

   - Las instancias deben tener una dirección IPv6 principal asignada para poder registrarse en un grupo de destino de IPv6.
   - AWS GovCloud (US) Region no admiten la asignación de una dirección IPv6 principal desde la consola. Debe usar la API para asignar direcciones IPv6 principales en s. AWS GovCloud (US) Region
6. Para anular el registro de instancias, seleccione la instancia y, a continuación, elija Anular registro.

Registro o anulación del registro de destinos por dirección IP

Destinos IPv4

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

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

No puede registrar las direcciones IP de otro Equilibrador de carga de aplicación en la misma VPC. Si el otro Equilibrador de carga de aplicación está en una VPC que está interconectada a la VPC del equilibrador de carga, puede registrar sus direcciones IP.

Destinos IPv6

- Las direcciones IP que registre deben estar dentro del bloque de CIDR de VPC o dentro de un bloque de CIDR de VPC emparejado.

Para registrar un destino o anular su registro mediante la dirección IP desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Para registrar direcciones IP, elija Registrar destinos. Para cada dirección IP, especifique la red, ingrese la dirección IP y el puerto y elija Incluir como pendiente debajo. Cuando haya terminado de especificar direcciones, elija Registrar destinos pendientes.
6. Para anular el registro de direcciones IP, selecciónelas y, a continuación, elija Anular registro. Si ha registrado muchas direcciones IP, puede que le resulte útil agregar un filtro o cambiar el orden.

Registrar o anular el registro de una función de Lambda

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

Cómo registrar o anular el registro de una función de Lambda mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Si no hay ninguna función de Lambda registrada, elija Registrar. Seleccione la función de Lambda y elija Registrar.
6. Para anular el registro de una función de Lambda, elija Anular registro Cuando se le pida que confirme, elija Deregister.

Registro o anulación del registro de destinos mediante la AWS CLI

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

Sesiones persistentes para Equilibrador de carga de aplicación

De forma predeterminada, un Equilibrador de carga de aplicación enruta cada solicitud de manera independiente a un destino registrado en función del algoritmo de equilibrio de carga elegido. Sin embargo, puede utilizar la característica de sesión persistente (también denominada afinidad de sesión) que permite que el equilibrador de carga vincule una sesión del usuario a una instancia concreta. Con ello se garantiza que todas las solicitudes de ese usuario durante la sesión se envían al mismo destino. Esta característica resulta útil para los servidores que mantienen información de estado, para ofrecer una experiencia de continuidad a los clientes. Para utilizar las sesiones persistentes, los clientes deben admitir las cookies.

Los equilibradores de carga de aplicaciones admiten cookies basadas en la duración y cookies basadas en aplicaciones. Las sesiones persistentes se habilitan para grupos de destino. Se puede usar una combinación de persistencia en función de la duración, persistencia en función de la aplicación y ausencia de persistencia en los grupos de destino.

La clave para administrar las sesiones persistentes consiste en determinar durante cuánto tiempo deberá direccionar el equilibrador de carga la solicitud del usuario a la misma instancia. Si la aplicación tiene su propia cookie de sesión, entonces puede usar la persistencia en función de la aplicación y la cookie de sesión del equilibrador de carga respeta la duración especificada por la cookie de sesión de la aplicación. Si la aplicación no tiene su propia cookie de sesión, entonces puede utilizar la persistencia en función de la duración para generar una cookie de sesión del equilibrador de carga con una duración especificada.

El contenido de estas cookies generadas por el equilibrador de carga se cifra mediante una clave rotativa. Las cookies generadas por el equilibrador de carga no se pueden descifrar ni modificar.

Para ambos tipos de persistencia, el Equilibrador de carga de aplicación restablece la caducidad de las cookies que genera después de cada solicitud. Si una cookie caduca, la sesión deja de ser persistente y el cliente debe eliminarla de su almacén de cookies.

Requisitos

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

Consideraciones

- Las sesiones persistentes no son compatibles si el equilibrio de carga entre zonas está deshabilitado. Si se intentan habilitar sesiones persistentes con el equilibrio de carga entre zonas deshabilitado, se producirá un error.
- En el caso de las cookies basadas en aplicaciones, los nombres de las cookies deben especificarse individualmente para cada grupo de destino. Sin embargo, en el caso de las cookies basadas en la duración, `AWSALB` es el único nombre que se utiliza en todos los grupos de destino.
- Si se utilizan varios niveles de equilibradores de carga de aplicaciones, puede habilitar sesiones persistentes en todas las capas con cookies basadas en aplicaciones. Sin embargo, con las cookies basadas en la duración, solo puede habilitar las sesiones persistentes en una capa, ya que `AWSALB` es el único nombre disponible.
- La persistencia en función de aplicaciones no funciona con grupos de destino ponderados.

- Si tiene una acción de reenvío con varios grupos de destino y uno o más de ellos tienen habilitadas las sesiones persistentes, debe habilitar la persistencia en el nivel del grupo de destino.
- WebSocket las conexiones son intrínsecamente fijas. Si el cliente solicita una actualización de la conexión WebSockets, el destino que devuelve un código de estado HTTP 101 para aceptar la actualización de la conexión es el destino utilizado en la WebSockets conexión. Una vez completada la WebSockets actualización, no se utiliza la adherencia basada en cookies.
- Los equilibradores de carga de aplicaciones utilizan el atributo `Expires` del encabezado de la cookie en lugar del atributo `Max-Age`.
- Los equilibradores de carga de aplicaciones no admiten valores de cookies codificados como URL.

Persistencia en función de la duración

La rigidez en función de la duración dirige las solicitudes al mismo destino de un grupo de destino mediante una cookie generada por el equilibrador de carga (`AWSALB`). La cookie se utiliza para asignar la sesión al destino. Si la aplicación no tiene su propia cookie de sesión, puede especificar su propia duración de persistencia y administrar durante cuánto tiempo el equilibrador de carga debe dirigir de manera consistente la solicitud del usuario al mismo destino.

Cuando un equilibrador de carga recibe una solicitud de un cliente por primera vez, la direcciona a un destino (según el algoritmo seleccionado) y genera una cookie denominada `AWSALB`. Codifica la información sobre el destino seleccionado, cifra la cookie y la incluye en la respuesta al cliente. La cookie generada por el equilibrador de carga tiene su propia caducidad de 7 días, que no se puede configurar.

En las solicitudes posteriores, el cliente debe incluir la cookie `AWSALB`. Cuando el equilibrador de carga recibe una solicitud de un cliente que contiene la cookie, la detecta y dirige la solicitud al mismo destino. Si la cookie está presente pero no se puede decodificar, o si hace referencia a un destino que cuyo registro se ha anulado o no está en buen estado, el equilibrador de carga selecciona un nuevo destino y actualiza la cookie con información sobre el nuevo destino.

En el caso de las solicitudes de intercambio de recursos entre orígenes (CORS), algunos navegadores requieren que se habilite la adherencia. `SameSite=None; Secure` Para admitir estos navegadores, el balanceador de cargas siempre genera una segunda cookie de adherencia`AWSALBCORS`, que incluye la misma información que la cookie de adherencia original, así como el atributo. `SameSite` Los clientes reciben ambas cookies, incluidas las solicitudes que no son de CORS.

Para habilitar la persistencia en función de la duración mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Edit attributes, lleve a cabo alguna de las siguientes operaciones:
   a. Seleccione Persistencia.
   b. Para Tipo de persistencia, seleccione Cookie generada por el equilibrador de carga.
   c. Para Duración de la persistencia, especifique un valor comprendido entre 1 segundo y 7 días.
   d. Elija Guardar cambios.

Para habilitar la adherencia basada en la duración, utilice el AWS CLI

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

Use el siguiente comando para habilitar la persistencia en función de la duración.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true
 Key=stickiness.lb_cookie.duration_seconds,Value=time-in-seconds
```

El resultado debería ser similar al siguiente ejemplo.

```
    {
       "Attributes": [
          ...
           {
                "Key": "stickiness.enabled",
                "Value": "true"
             },
             {
                 "Key": "stickiness.lb_cookie.duration_seconds",
                 "Value": "86500"
```

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

Persistencia en función de la aplicación

La persistencia en función de la aplicación le brinda la flexibilidad de establecer sus propios criterios para determinar la persistencia a los destinos del cliente. Cuando se habilita la persistencia en función de las aplicaciones, el equilibrador de carga dirige la primera solicitud a un destino del grupo de destino en función del algoritmo elegido. Se espera que el destino establezca una cookie de aplicación personalizada que coincida con la cookie configurada en el equilibrador de carga para permitir la persistencia. Esta cookie personalizada puede incluir cualquiera de los atributos de cookie requeridos por la aplicación.

Cuando el Equilibrador de carga de aplicación recibe la cookie de aplicación personalizada del destino, genera automáticamente una nueva cookie de aplicación cifrada para capturar la información de persistencia. Esta cookie de aplicación generada por el equilibrador de carga captura la información sobre la persistencia de cada grupo de destino que tiene habilitada la persistencia en función de aplicaciones.

La cookie de aplicación generada por el equilibrador de carga no copia los atributos de la cookie personalizada establecida por el destino. Tiene su propia caducidad de 7 días, que no se puede configurar. En la respuesta al cliente, el Equilibrador de carga de aplicación solo valida el nombre con el que se configuró la cookie personalizada a nivel del grupo de destino y no el valor ni el atributo de caducidad de la cookie personalizada. Siempre que el nombre coincida, el equilibrador de carga envía ambas cookies, la cookie personalizada establecida por el destino y la cookie de aplicación generada por el equilibrador de carga, en la respuesta al cliente.

En las solicitudes posteriores, los clientes tienen que devolver ambas cookies para mantener la persistencia. El equilibrador de carga descifra la cookie de la aplicación y comprueba si el tiempo de permanencia configurado sigue siendo válido. Luego, utiliza la información de la cookie para enviar la solicitud al mismo destino dentro del grupo de destino con el fin de mantener la persistencia. El equilibrador de carga también envía por proxy la cookie de la aplicación personalizada al destino sin inspeccionarla ni modificarla. En las respuestas posteriores, se restablecen la fecha de caducidad de la cookie de aplicación generada por el equilibrador de carga y el tiempo de permanencia configurado en el equilibrador de carga. Para mantener la persistencia entre el cliente y el destino, la caducidad de la cookie y el tiempo de persistencia no deben llegar a su fin.

Si se produce un error en una instancia o esta pasa a encontrarse en mal estado, el equilibrador de carga deja de enrutar las solicitudes a esa instancia y elige una nueva en buen estado en función del algoritmo de equilibrio de carga existente. El equilibrador de carga trata la sesión como si estuviera "adherida" a la nueva instancia en buen estado y continúa direccionando las solicitudes a esa instancia aunque la instancia que sufrió el error vuelva a estar en buen estado.

En el caso de las solicitudes de intercambio de recursos entre orígenes (CORS), el equilibrador de carga añade los atributos `SameSite=None; Secure` a la cookie de la aplicación generada por el equilibrador de carga solo si la versión del agente de usuario es Chromium80 o superior.

Debido a que la mayoría de los navegadores limitan una cookie a 4 KB de tamaño, el equilibrador de carga fragmenta las cookies de más de 4 KB en varias cookies. Los equilibradores de carga de aplicaciones admiten cookies de hasta 16 KB y, por lo tanto, pueden crear hasta 4 particiones para enviarlos al cliente. El nombre de la cookie de la aplicación que ve el cliente comienza por «AWSALBAPP-» e incluye un número de fragmento. Por ejemplo, si el tamaño de la cookie es de 0 a 4 K, el cliente ve AWSALBAPP -0. Si el tamaño de la cookie es de 4 a 8 k, el cliente ve AWSALBAPP -0 y -1, y AWSALBAPP así sucesivamente.

Para habilitar las sesiones persistentes controladas por la aplicación desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. En la página Edit attributes, lleve a cabo alguna de las siguientes operaciones:

    a. Seleccione Persistencia.

    b. Para el tipo de persistencia, seleccione Cookie en función de aplicaciones.

    c. Para Duración de la persistencia, especifique un valor comprendido entre 1 segundo y 7 días.

    d. En Nombre de la cookie de la aplicación, ingrese un nombre para la cookie en función de la aplicación.

    No utilice `AWSALB`, `AWSALBAPP` o `AWSALBTG` para el nombre de la cookie; están reservados para el uso del equilibrador de carga.

    e. Elija Guardar cambios.

Para habilitar la adherencia basada en aplicaciones, utilice el AWS CLI

Utilice el comando modify-target-group-attributes con los atributos siguientes:

- `stickiness.enabled`
- `stickiness.type`
- `stickiness.app_cookie.cookie_name`
- `stickiness.app_cookie.duration_seconds`

Use el siguiente comando para habilitar la persistencia en función de aplicaciones.

```
aws elbv2 modify-target-group-attributes --target-group-arn ARN --attributes
 Key=stickiness.enabled,Value=true Key=stickiness.type,Value=app_cookie
 Key=stickiness.app_cookie.cookie_name,Value=my-cookie-name
 Key=stickiness.app_cookie.duration_seconds,Value=time-in-seconds
```

El resultado debería ser similar al siguiente ejemplo.

```
      {
          "Attributes": [
              ...
              {
                  "Key": "stickiness.enabled",
                  "Value": "true"
              },
              {
                  "Key": "stickiness.app_cookie.cookie_name",
                  "Value": "MyCookie"
              },
              {
                  "Key": "stickiness.type",
                  "Value": "app_cookie"
              },
              {
                  "Key": "stickiness.app_cookie.duration_seconds",
                  "Value": "86500"
              },
              ...
          ]
       }
```

Reequilibrado manual

Al escalar verticalmente, si el número de destinos aumenta considerablemente, existe la posibilidad de que la carga se distribuya de forma desigual debido a la persistencia. En este escenario, puede reequilibrar la carga sobre los destinos mediante las dos opciones siguientes:

- Establezca un vencimiento en la cookie generada por la aplicación que sea anterior a la fecha y la hora en curso. Esto evitará que los clientes envíen la cookie al Equilibrador de carga de aplicación, lo que reiniciará el proceso de establecimiento de la persistencia.
- Establezca una duración muy corta en la configuración de persistencia en función de aplicaciones del equilibrador de carga, por ejemplo, 1 segundo. Esto obliga al Equilibrador de carga de aplicación a restablecer la persistencia incluso si la cookie establecida por el destino no ha caducado.

Funciones de Lambda como destino

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

Límites

- La función de Lambda y el grupo de destino deben estar en la misma cuenta y en la misma región.
- El tamaño máximo del cuerpo de la solicitud que puede enviar a una función de Lambda es de 1 MB. Para ver límites de tamaño relacionados, consulte Límites de los encabezados HTTP.
- El tamaño máximo del JSON de respuesta que la función de Lambda puede enviar es de 1 MB.
- WebSockets no son compatibles. Las solicitudes de actualización se rechazan con el código HTTP 400.
- No se admiten las Zonas locales.
- No se admiten los pesos objetivo automáticos (ATW).

Contenido

- Preparar la función de Lambda
- Creación de un grupo de destino para la función de Lambda
- Recibir eventos del equilibrador de carga
- Responder al equilibrador de carga
- Encabezados de varios valores
- Deshabilitar las comprobaciones de estado
- Anular el registro de la función de Lambda

Para ver una demostración, consulte Destino de Lambda en Equilibrador de carga de aplicación.

Preparar la función de Lambda

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

Permisos para invocar la función de Lambda

Si crea el grupo de destino y registra la función de Lambda utilizando la AWS Management Console, la consola añade los permisos necesarios a la política de su función de Lambda en su nombre. De lo contrario, después de crear el grupo objetivo y registrar la función mediante el AWS CLI, debe utilizar el comando add-permission para conceder a Elastic Load Balancing el permiso para invocar la función Lambda. Le recomendamos que use las claves de condición `aws:SourceAccount` y `aws:SourceArn` para restringir la invocación de la función al grupo de destino especificado. Para obtener más información, consulte El problema del suplente confuso en la Guía del usuario de IAM.

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

Control de versiones de funciones de Lambda

Puede registrar una sola función de Lambda por grupo de destino. Para asegurarse de que puede cambiar la función de Lambda y de que el equilibrador de carga siempre invoque la versión actual de la función de Lambda, cree un alias de función e incluya el alias en el ARN de la función cuando

registre la función de Lambda en el equilibrador de carga. Para obtener más información, consulte Control de versiones y alias de las funciones AWS Lambda y Cambio de tráfico mediante alias en la Guía del desarrollador de AWS Lambda .

Tiempo de espera de la función

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

Creación de un grupo de destino para la función de Lambda

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

Cómo crear un grupo de destino y registrar la función de Lambda mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija Crear grupo de destino.
4. En Seleccionar un destino, elija Función de Lambda.
5. En Target group name, escriba el nombre del nuevo grupo de destino.
6. (Opcional) Para habilitar las comprobaciones, elija Comprobación de estado, Habilitar.
7. (Opcional) Agregue una o varias etiquetas, como se indica a continuación:
   a. Expanda la sección Etiquetas.
   b. Seleccione Agregar etiqueta.
   c. Escriba la clave y el valor de la etiqueta.
8. Elija Siguiente.
9. Especifique una sola función de Lambda u omita este paso y especifique una función de Lambda más adelante.
10. Elija Crear grupo de destino.

Cómo crear un grupo de destino y registrar la función de Lambda mediante la AWS CLI

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

Recibir eventos del equilibrador de carga

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

Si el encabezado `content-encoding` está presente, el equilibrador de carga Base64 codifica el cuerpo y establece `isBase64Encoded` en `true`.

Si el encabezado `content-encoding` no está presente, la codificación en Base64 depende del tipo de contenido. Si el tipo de contenido es uno de los siguientes, el equilibrador de carga envía el cuerpo a la función de Lambda tal como está y establece `isBase64Encoded` en `false`: text/*, application/json, application/javascript y application/xml. Para todos los demás tipos, el equilibrador de carga codifica en Base64 el cuerpo y establece `isBase64Encoded` en `true`.

El siguiente es un evento de ejemplo.

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

```
        "x-forwarded-port": "443",
        "x-forwarded-proto": "https"
    },
    "isBase64Encoded": false,
    "body": "request_body"
}
```

Responder al equilibrador de carga

La respuesta de la función de Lambda debe incluir el estado de codificación en Base64, el código de estado y los encabezados. Puede omitir el cuerpo.

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

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

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

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

Para conocer las plantillas de la función de Lambda que funcionan con los equilibradores de carga de aplicaciones, consulte application-load-balancer-serverless-app en github. También puede abrir la consola de Lambda, elegir Aplicaciones, Crear una aplicación y seleccionar una de las siguientes opciones de entre AWS Serverless Application Repository:

- ALB-Lambda-Target- S3 UploadFileto
- ALB-Lambda-objetivo- BinaryResponse
- ALB-Lambda-Target- IP WhatisMy

Encabezados de varios valores

Si las solicitudes de un cliente o las respuestas de una función de Lambda incluyen encabezados con varios valores o el mismo encabezado varias veces, o parámetros de consulta con varios valores para la misma clave, puede habilitar la compatibilidad con la sintaxis de encabezados de varios valores. Después de habilitar encabezados de varios valores, los encabezados y los parámetros de consulta intercambiados entre el equilibrador de carga y la función de Lambda utilizan matrices en lugar de cadenas. Si no habilita la sintaxis de encabezado de varios valores y un parámetro de encabezado o consulta tiene varios valores, el equilibrador de carga utiliza el último valor que reciba.

Contenido

- Solicitudes con encabezados de varios valores
- Respuestas con encabezados de varios valores
- Habilitar encabezados de varios valores

Solicitudes con encabezados de varios valores

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

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

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

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

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

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

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

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

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

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

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

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

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

Si los parámetros de consulta están codificados en URL, el equilibrador de carga no los decodifica. Debe decodificarlos en la función de Lambda.

Respuestas con encabezados de varios valores

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

Con el formato predeterminado, puede especificar una única cookie:

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

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

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

Es posible que el equilibrador de carga envíe los encabezados al cliente en un orden diferente al especificado en la carga útil de respuesta de Lambda. Por lo tanto, no espere que los encabezados se devuelvan en un orden específico.

Habilitar encabezados de varios valores

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

Para habilitar los encabezados de varios valores con la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Atributos, seleccione Editar.
5. Seleccione o desactive los encabezados con varios valores.
6. Elija Guardar cambios.

Para habilitar los encabezados con varios valores mediante el AWS CLI

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

Deshabilitar las comprobaciones de estado

De forma predeterminada, las comprobaciones de estado están deshabilitadas para los grupos de destino de tipo `lambda`. Puede habilitar las comprobaciones de estado a fin de implementar la conmutación por error de DNS con Amazon Route 53. La función de Lambda puede comprobar el

estado de un servicio posterior antes de responder a la solicitud de comprobación de estado. Si la respuesta de la función de Lambda indica un error en la comprobación de estado, este error se pasa a Route 53. Puede configurar Route 53 para que realice una conmutación por error a una pila de aplicaciones de reserva.

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

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

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

Para habilitar las comprobaciones de estado de un grupo objetivo mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Detalles del grupo, en la sección Configuración de comprobación de estado, seleccione Editar.
5. En Comprobación de estado, seleccione Habilitar.

6. Elija Guardar cambios.

Para habilitar las comprobaciones de estado de un grupo objetivo mediante el AWS CLI

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

Anular el registro de la función de Lambda

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

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

Para anular el registro de la función Lambda mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Destinos, elija Anular registro.
5. Cuando se le pida que confirme, elija Deregister.

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

Use el comando deregister-targets.

Etiquetas para su grupo de destino

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

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

Cuando ya no necesite una etiqueta, puede eliminarla.

Restricciones

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

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

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar su página de detalles.
4. En la pestaña Etiquetas, elija Administrar etiquetas y realice una o varias de las acciones siguientes:
   a. Para actualizar una etiqueta, ingrese valores nuevos para Clave y Valor.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.
5. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de un grupo objetivo mediante el AWS CLI

Utilice los comandos add-tags y remove-tags.

Eliminación de un grupo de destino

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

Para eliminar un grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Seleccione el grupo de destino y elija Actions, Delete.
4. Cuando se le indique que confirme, seleccione Sí, borrar.

Para eliminar un grupo objetivo mediante el AWS CLI

Utilice el comando delete-target-group.

Monitorización de los equilibradores de carga de aplicaciones

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

CloudWatch métricas

Puedes usar Amazon CloudWatch para recuperar estadísticas sobre puntos de datos para tus balanceadores de carga y objetivos como un conjunto ordenado de datos de series temporales, conocidos como métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte CloudWatch métricas para su Application Load Balancer.

Registros de acceso

Puede utilizar los registros de acceso para capturar información detallada sobre las solicitudes realizadas al equilibrador de carga y almacenarla en archivos de registro en Amazon S3. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar problemas en los destinos. Para obtener más información, consulte Registros de acceso del Equilibrador de carga de aplicación.

Registros de conexión

Puede usar los registros de conexión para capturar los atributos de las solicitudes enviadas a su balanceador de carga y almacenarlos como archivos de registro en Amazon S3. Puede usar estos registros de conexión para determinar la dirección IP y el puerto del cliente, la información del certificado del cliente, los resultados de la conexión y los cifrados TLS que se utilizan. Luego, estos registros de conexión se pueden usar para revisar los patrones de solicitudes y otras tendencias. Para obtener más información, consulte Registros de conexión para su Application Load Balancer.

Rastreo de solicitudes

Puede utilizar el rastreo de solicitudes para realizar un seguimiento de las solicitudes HTTP. El equilibrador de carga agrega un encabezado con un identificador de rastreo a cada solicitud que recibe. Para obtener más información, consulte Solicite un rastreo de equilibrador de carga de aplicaciones..

CloudTrail registros

Se puede utilizar AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a la API de Elastic Load Balancing y almacenarlas como archivos de registro en Amazon S3. Puede usar estos CloudTrail registros para determinar qué llamadas se realizaron, la dirección IP de origen de la llamada, quién realizó la llamada, cuándo se realizó la llamada, etc. Para obtener más información, consulte Registro de llamadas a la API del Equilibrador de carga de aplicación mediante AWS CloudTrail.

CloudWatch métricas para su Application Load Balancer

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

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una CloudWatch alarma para supervisar una métrica específica e iniciar una acción (como enviar una notificación a una dirección de correo electrónico) si la métrica se encuentra fuera de lo que considera un rango aceptable.

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

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

Contenido

- Métricas del Equilibrador de carga de aplicación
- Dimensiones de las métricas de los equilibradores de carga de aplicaciones
- Estadísticas para métricas del Equilibrador de carga de aplicación
- Consulta CloudWatch las métricas de tu balanceador de cargas

Métricas del Equilibrador de carga de aplicación

- Equilibradores de carga
- Destinos
- Estado del grupo de destino
- Funciones de Lambda
- Autenticación del usuario

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

Métrica	Descripción
`ActiveConnectionCount`	El número total de conexiones TCP simultáneas activas desde los clientes al equilibrador de carga y desde el equilibrador de carga a los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`AnomalousHostCount`	El número de hosts detectados con anomalías. Criterios del informe: se informa siempre Estadísticas: las estadísticas más útiles son `Average`, `Minimum` y `Maximum`. Dimensiones • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
`ClientTLSNegotiationErrorCount`	El número de conexiones TLS iniciadas por el cliente que no establecieron una sesión con el equilibrador de carga debido a un error de TLS. Las posibles causas incluyen la falta de coincidencia de los cifrados o protocolos o que el cliente no pudo verificar el certificado del servidor y cerró la conexión. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ConsumedLCUs`	El número de unidades de capacidad del equilibrador de carga (LCU) usadas por el equilibrador de carga. Se paga por el número de LCU usadas a la hora. Para obtener más información, consulte Precios de Elastic Load Balancing. Criterios del informe: se informa siempre Estadísticas: todas Dimensiones • `LoadBalancer`
`DesyncMitigationMode_NonCompliant_Request_Count`	El número de solicitudes que no cumplen con RFC 7230. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
`DroppedInvalidHeaderRequestCount`	Número de solicitudes en las que el equilibrador de carga eliminó encabezados HTTP con campos de encabezado que no son válidos antes de enrutar la solicitud. El equilibrador de carga quita estos encabezados solo si el atributo `routing.http.drop_invalid_header_fields.enabled` está establecido en `true`. Criterios del informe: hay un valor distinto de cero Estadísticas: todas Dimensiones • `AvailabilityZone` , `LoadBalancer`
`MitigatedHostCount`	El número de objetivos que se están mitigando. Criterios del informe: se informa siempre Estadísticas: las estadísticas más útiles son `Average`, `Minimum` y `Maximum`. Dimensiones • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
ForwardedInvalidHeaderRequestCount	Número de solicitudes enrutadas por el equilibrador de carga que tenían encabezados HTTP con campos de encabezado que no son válidos. El equilibrador de carga reenvía las solicitudes con estos encabezados solo si el atributo routing.http.drop_invalid_header_fields.enabled está establecido en false. Criterios del informe: se informa siempre Estadísticas: todas Dimensiones • AvailabilityZone , LoadBalancer
GrpcRequestCount	El número de solicitudes gRPC que se procesaron por IPv4 e IPv6. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil esSum. Minimum, Maximum y Average todas devuelven 1. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
HTTP_Fixed_Response_Count	El número de acciones de respuesta fija que se han realizado correctamente. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
HTTP_Redirect_Count	El número de acciones de redireccionamiento que se han realizado correctamente. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
HTTP_Redirect_Url_Limit_Exceeded_Count	El número de acciones de redireccionamiento que no se han podido completar porque la URL en el encabezado de la ubicación de respuesta es mayor que 8 K. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
HTTPCode_ELB_3XX_Count	El número de códigos de redireccionamiento de HTTP 3XX que proceden del equilibrador de carga. Este recuento no incluye los códigos de respuesta generados por los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
HTTPCode_ELB_4XX_Count	El número de códigos de error del cliente HTTP 4XX que proceden del equilibrador de carga. Este recuento no incluye los códigos de respuesta generados por los destinos. Los errores del cliente se generan cuando las solicitudes no tienen el formato correcto o están incompletas. El destino no recibió estas solicitudes, excepto en el caso en que el equilibrador de carga devuelve un código de error HTTP 460. Este número no incluye los códigos de respuesta generados por los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. `Minimum`, `Maximum` y `Average` todas devuelven 1. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
HTTPCode_ELB_5XX_Count	El número de códigos de error del servidor HTTP 5XX que proceden del equilibrador de carga. Este número no incluye los códigos de respuesta generados por los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. `Minimum`, `Maximum` y `Average` todas devuelven 1. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
HTTPCode_ELB_500_Count	El número de códigos de error del servidor HTTP 500 que proceden del equilibrador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
HTTPCode_ELB_502_Count	El número de códigos de error del servidor HTTP 502 que proceden del equilibrador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
HTTPCode_ELB_503_Count	El número de códigos de error del servidor HTTP 503 que proceden del equilibrador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
HTTPCode_ELB_504_Count	El número de códigos de error del servidor HTTP 504 que proceden del equilibrador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
IPv6ProcessedBytes	El número total de bytes procesados por el equilibrador de carga a través de IPv6. Este recuento se incluye en ProcessedBytes . Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
IPv6RequestCount	El número de solicitudes IPv6 recibidas por el equilibrador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil esSum. Minimum, Maximum y Average todas devuelven 1. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
NewConnectionCount	El número total de conexiones TCP nuevas establecidas desde los clientes al equilibrador de carga y desde el equilibrador de carga a los destinos. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
NonStickyRequestCount	El número de solicitudes para las que equilibrador de carga eligió un nuevo destino porque no pudo utilizar una sesión persistente existente. Por ejemplo, la solicitud era la primera solicitud de un nuevo cliente y no había ninguna cookie de persistencia, se presentó una cookie de persistencia pero no se especificó un destino registrado con este grupo de destino, la cookie de persistencia tenía un formato incorrecto o había caducado o un error interno impidió que el equilibrador de carga leyese la cookie de persistencia. Reporting criteria (Criterios del informe): la persistencia está habilitada en el grupo de destino. Estadísticas: la única estadística relevante es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
`ProcessedBytes`	El número total de bytes procesados por el equilibrador de carga a través de IPv4 e IPv6. Este recuento incluye el tráfico entrante y saliente de los clientes y las funciones de Lambda, así como el tráfico de un proveedor de identidad (IdP) si la autenticación de usuarios está habilitada. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedConnectionCount`	El número de conexiones que se rechazaron porque el equilibrador de carga alcanzó el número máximo de conexiones. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
RequestCount	El número de solicitudes que se procesaron por IPv4 e IPv6. Esta métrica solo se incrementa para las solicitudes en las que el nodo del equilibrador de carga pudo elegir un destino. Las solicitudes que se rechazan antes de elegir un destino no se reflejan en esta métrica. Criterios del informe: se informa siempre Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • LoadBalancer , AvailabilityZone • LoadBalancer , TargetGroup • LoadBalancer , AvailabilityZone , TargetGroup
RuleEvaluations	El número de reglas procesadas por el equilibrador de carga dado el número medio de solicitudes por hora. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer

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

Métrica	Descripción
HealthyHostCount	El número de destinos que se considera que están en buen estado. Criterios del informe: indica si se han activado las comprobaciones de estado

Métrica	Descripción
	Estadísticas: las estadísticas más útiles son `Average`, `Minimum` y `Maximum`. Dimensiones • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`
`HTTPCode_Target_2XX_Count` , `HTTPCode_Target_3XX_Count` , `HTTPCode_Target_4XX_Count` , `HTTPCode_Target_5XX_Count`	El número de códigos de respuesta HTTP generados por los destinos. Este número no incluye los códigos de respuesta generados por el equilibrador de carga. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es`Sum`. `Minimum`, `Maximum` y `Average` todas devuelven 1. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
`RequestCountPerTarget`	El número medio de solicitudes por objetivo, en un grupo objetivo. Debe especificar el grupo de destino mediante la dimensión `TargetGroup` . Esta métrica no se aplica si el destino es una función de Lambda. Este recuento utiliza el número total de solicitudes recibidas por el grupo objetivo, dividido por el número de objetivos en buen estado del grupo objetivo. Si no hay objetivos en buen estado en el grupo objetivo, se indica el número total de objetivos. Criterios del informe: se informa siempre Estadísticas: la única estadística válida es `Sum`. Esto representa la media, no la suma. Dimensiones • `TargetGroup` • `TargetGroup` , `AvailabilityZone` • `LoadBalancer` , `TargetGroup` • `LoadBalancer` , `AvailabilityZone` , `TargetGroup`
`TargetConnectionErrorCount`	El número de conexiones que no se establecieron correctamente entre el equilibrador de carga y el destino. Esta métrica no se aplica si el destino es una función de Lambda. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup` , `LoadBalancer` • `TargetGroup` , `AvailabilityZone` , `LoadBalancer`

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

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

El espacio de nombres `AWS/ApplicationELB` incluye las siguientes métricas para el estado del grupo de destino. Para obtener más información, consulte the section called “Estado del grupo de destino”.

Métrica	Descripción
`HealthyStateDNS`	La cantidad de zonas que cumplen los requisitos de estado correcto del DNS. Estadísticas: la estadística más útil es `Min`. Dimensiones • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`HealthyStateRouting`	La cantidad de zonas que cumplen los requisitos de estado correcto del enrutamiento. Estadísticas: la estadística más útil es `Min`.

Métrica	Descripción
	Dimensiones • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`UnhealthyRoutingRequestCount`	La cantidad de solicitudes que se enrutan mediante la acción de conmutación por error de enrutamiento (apertura por error). Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`UnhealthyStateDNS`	La cantidad de zonas que no cumplen los requisitos de estado correcto del DNS y, por lo tanto, se marcaron como zonas en mal estado en el DNS. Estadísticas: la estadística más útil es `Min`. Dimensiones • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`UnhealthyStateRouting`	La cantidad de zonas que no cumplen los requisitos de estado correcto del enrutamiento y, por lo tanto, el equilibrador de carga distribuye el tráfico a todos los destinos de la zona, incluidos los destinos en mal estado. Estadísticas: la estadística más útil es `Min`. Dimensiones • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`

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

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

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

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

Métrica	Descripción
`ELBAuthError`	El número de autenticaciones de usuario que no se han podido completar porque se ha configurado de manera incorrecta una acción de autenticación o el equilibrador de carga no ha podido establecer una conexión con el IdP o no ha podido completar el flujo de autenticación debido a un error interno. Para obtener los códigos de los motivos de error, consulte el campo error_reason del registro de acceso. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthFailure`	El número de autenticaciones de usuario que no se han podido completar debido a que el IdP ha denegado el acceso al usuario o se ha utilizado varias veces un código de autorización. Para obtener los códigos de los motivos de error, consulte el campo error_reason del registro de acceso.

Métrica	Descripción
	Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthLatency`	El tiempo transcurrido, en milisegundos, en solicitar al IdP el token de ID y la información del usuario. Si se produce un error en una o en varias de estas operaciones, este es el tiempo transcurrido hasta el error. Criterios del informe: hay un valor distinto de cero Estadísticas: todas las estadísticas son relevantes. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthRefreshTokenSuccess`	El número de veces que el equilibrador de carga actualizó correctamente las notificaciones de usuario con un token de actualización proporcionado por el proveedor de identidad. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
`ELBAuthSuccess`	El número de acciones de autenticación que se han realizado correctamente. Esta métrica se incrementa al final del flujo de trabajo de autenticación, después de que el equilibrador de carga haya recuperado las notificaciones de usuario del IdP. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ELBAuthUserClaimsSizeExceeded`	El número de veces que un proveedor de identidad devolvió las notificaciones de usuario con un tamaño superior a 11 K. Criterios del informe: hay un valor distinto de cero Estadísticas: la única estadística relevante es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Dimensiones de las métricas de los equilibradores de carga de aplicaciones

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

Dimensión	Descripción
`AvailabilityZone`	Filtra los datos de métricas por zona de disponibilidad.
`LoadBalancer`	Filtra los datos de métricas por equilibrador de carga. Especifique el equilibrador de carga del modo siguiente: app/nombre-balanceador-

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

Estadísticas para métricas del Equilibrador de carga de aplicación

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

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

Le recomendamos que controle los `UnHealthyHostCount` distintos de cero en la estadística de `Minimum` y que active la alarma si los valores son distintos de cero en más de un punto de datos. El uso de `Minimum` detectará si cada nodo y zona de disponibilidad del equilibrador de carga considera que los destinos no tienen el estado correcto. La alarma activada en `Average` o `Maximum` es útil si quiere recibir alertas sobre posibles problemas, por lo que recomendamos a los clientes que revisen esta métrica e investiguen los casos en los que los valores sean distintos a cero. La mitigación automática de los errores se puede realizar siguiendo las prácticas recomendadas de utilizar la comprobación de estado del equilibrador de carga en Amazon EC2 Auto Scaling o Amazon Elastic Container Service (Amazon ECS).

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

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

Un percentil indica el peso relativo de un valor en un conjunto de datos. Puede especificar cualquier percentil con hasta dos decimales (por ejemplo, p95.45). Por ejemplo, el percentil 95 significa que el 95 % de los datos está por debajo de este valor y el 5 % está por encima de él. Los percentiles se suelen utilizar para aislar anomalías. Por ejemplo, supongamos que una aplicación tarda entre 1 y 2 ms en atender la mayoría de las solicitudes desde una caché; pero que tarda 100-200 ms si la caché está vacía. El máximo refleja el caso más lento, de unos 200 ms. El promedio no indica la distribución de los datos. Los percentiles proporcionan una visión más significativa del rendimiento de la aplicación. Al usar el percentil 99 como disparador o CloudWatch alarma de Auto Scaling, puede tener como objetivo que no más del 1 por ciento de las solicitudes tarden más de 2 ms en procesarse.

Consulta CloudWatch las métricas de tu balanceador de cargas

Puede ver las CloudWatch métricas de sus balanceadores de carga mediante la consola Amazon EC2. 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, puede ver las métricas de su balanceador de carga mediante la consola. CloudWatch

Para consultar las métricas desde la consola de

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Para ver las métricas filtradas por grupo de destino, haga lo siguiente:
   a. En el panel de navegación, elija Target Groups.
   b. Seleccione el grupo de destino y, a continuación, elija la pestaña Monitoring.
   c. (Opcional) Para filtrar los resultados por tiempo, seleccione un intervalo de tiempo en Showing data for.

d. Para obtener una vista más amplia de una misma métrica, seleccione su gráfico.

3. Para ver las métricas filtradas por equilibrador de carga, haga lo siguiente:

   a. En el panel de navegación, seleccione Equilibradores de carga.

   b. Seleccione el equilibrador de carga y, a continuación, elija la pestaña Monitorizar.

   c. (Opcional) Para filtrar los resultados por tiempo, seleccione un intervalo de tiempo en Showing data for.

   d. Para obtener una vista más amplia de una misma métrica, seleccione su gráfico.

Para ver las métricas mediante la consola CloudWatch

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione ApplicationELB espacio de nombre.
4. (Opcional) Para ver una métrica en todas las dimensiones, ingrese su nombre en el campo de búsqueda.
5. (Opcional) Para filtrar por dimensión, seleccione una de las siguientes opciones:

   - Para mostrar solamente las métricas registradas para los equilibradores de carga, elija Por métrica de AppELB. Para ver las métricas de un solo equilibrador de carga, escriba su nombre en el campo de búsqueda.
   - Para mostrar solamente las métricas registradas para los grupos de destino, elija Por métrica de AppELB, de TG. Para ver las métricas de un solo grupo de destino, escriba su nombre en el campo de búsqueda.
   - Para mostrar solamente las métricas registradas para los equilibradores de carga por zona de disponibilidad, elija Por métrica de AppELB, de AZ. Para ver las métricas de un solo equilibrador de carga, escriba su nombre en el campo de búsqueda. Para ver las métricas de una sola zona de disponibilidad, escriba su nombre en el campo de búsqueda.
   - Para mostrar solamente las métricas registradas para los equilibradores de carga por zona de disponibilidad y el grupo de destino, elija Por métricas de AppELB, de AZ, de TG. Para ver las métricas de un solo equilibrador de carga, escriba su nombre en el campo de búsqueda. Para ver las métricas de un solo grupo de destino, escriba su nombre en el campo de búsqueda. Para ver las métricas de una sola zona de disponibilidad, escriba su nombre en el campo de búsqueda.

Para ver las métricas mediante el AWS CLI

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

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

Para obtener las estadísticas de una métrica mediante el AWS CLI

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

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

A continuación, se muestra un ejemplo de la salida:

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

Registros de acceso del Equilibrador de carga de aplicación

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

Los registros de acceso son una característica opcional de Elastic Load Balancing que está desactivada de forma predeterminada. Una vez que se han habilitado los registros de acceso del equilibrador de carga, Elastic Load Balancing captura los registros y los almacena en el bucket de Amazon S3 que haya especificado como archivos comprimidos. Puede deshabilitar los registros de acceso en cualquier momento.

Se cobran los costos de almacenamiento en Amazon S3, pero no el ancho de banda que Elastic Load Balancing utilice para enviar los archivos de registros a Amazon S3. Para obtener más información acerca de los costos de almacenamiento, consulte Precios de Amazon S3.

Contenido

- Archivos de registro de acceso
- Entradas de los registros de acceso
- Ejemplo de entradas de registro
- Procesamiento de archivos de registro de acceso
- Registros de acceso del Equilibrador de carga de aplicación
- Registros de acceso deshabilitados del Equilibrador de carga de aplicación

Archivos de registro de acceso

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

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

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

bucket

Nombre del bucket de S3.

prefix

(Opcional) El prefijo (jerarquía lógica) del bucket. El prefijo que especifique no debe incluir la cadena `AWSLogs`. Para obtener más información, consulte Organizar objetos con prefijos.

`AWSLogs`

Agregamos la parte del nombre de archivo que comienza por `AWSLogs` después del nombre del bucket y el prefijo que especifique.

aws-account-id

El ID de AWS cuenta del propietario.

region

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

aaaa/mm/dd

La fecha de entrega del log.

load-balancer-id

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

end-time

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

ip-address

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

random-string

Una cadena generada aleatoriamente por el sistema.

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

```
s3://my-bucket/my-prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2022/05/01/123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

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

```
s3://my-bucket/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2022/05/01/123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

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

Entradas de los registros de acceso

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

Cada entrada de registro contiene los detalles de una sola solicitud (o conexión en su caso WebSockets) realizada al balanceador de cargas. WebSocketsEn efecto, una entrada se escribe solo después de cerrar la conexión. Si la conexión actualizada no se puede establecer, la entrada será la misma que para una solicitud HTTP o HTTPS.

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

Contenido

- Sintaxis
- Medidas tomadas
- Motivos de la clasificación

- Códigos de motivo de error

Sintaxis

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

Campo	Descripción
type	Tipo de solicitud o conexión. Los valores posibles son los siguientes (haga caso omiso de todos los demás valores): • `http` — HTTP • `https` — HTTP sobre TLS • `h2` — HTTP/2 sobre SSL/TLS • `grpcs` — gRPC sobre TLS • `ws` — WebSockets • `wss`— a WebSockets través de TLS
hora	Hora a la que el equilibrador de carga generó una respuesta al cliente, en formato ISO 8601. Pues WebSockets, este es el momento en que se cierra la conexión.
elb	ID de recurso del equilibrador de carga. Al analizar entradas de registro de acceso, tenga en cuenta que los ID de recursos pueden contener barras diagonales (/).
client:port	Dirección IP y puerto del cliente solicitante. Si hay un proxy delante del equilibrador de carga, este campo contiene la dirección IP del proxy.
target:port	Dirección IP y puerto del destino que procesó esta solicitud. Si el cliente no envió una solicitud completa, el equilibrador de carga no puede enviar la solicitud a un destino, en cuyo caso este valor se establece en -.

Campo	Descripción
	Si el destino es una función de Lambda, este valor se establece en -. Si la solicitud está bloqueada por AWS WAF, este valor se establece en - y el valor de elb_status_code se establece en 403.
request_processing_time	Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el equilibrador de carga recibió la solicitud hasta que se la envió a un destino. Este valor también se establece en -1 si el equilibrador de carga no consigue enviar la solicitud a un destino. Esto puede ocurrir si el destino cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto. Este valor también se puede establecer en -1 si el destino registrado no responde antes de que se agote el tiempo de inactividad. Si AWS WAF está habilitada para su Application Load Balancer o el tipo de destino es una función Lambda, se tendrá en cuenta el tiempo que tarda el cliente en enviar los datos necesarios para las solicitudes POST. `request_processing_time`
target_processing_time	Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el equilibrador de carga envió la solicitud a un destino hasta que este comenzó a enviar los encabezados de la respuesta. Este valor también se establece en -1 si el equilibrador de carga no consigue enviar la solicitud a un destino. Esto puede ocurrir si el destino cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto. Este valor también se puede establecer en -1 si el destino registrado no responde antes de que se agote el tiempo de inactividad. Si no AWS WAF está activado para su Application Load Balancer, se tendrá en cuenta el tiempo que tarda el cliente en enviar los datos necesarios para las solicitudes POST. `target_processing_time`

Campo	Descripción
response_processing_time	Tiempo total (en segundos, con precisión de milisegundo) transcurrido desde que el equilibrador de carga recibió el encabezado de respuesta del destino hasta que comenzó a enviar la respuesta al cliente. Esto incluye tanto el tiempo de cola en el equilibrador de carga como tiempo de adquisición de la conexión entre el equilibrador de carga y el cliente. Este valor se establece en -1 si el equilibrador de carga no recibe una respuesta de un destino. Esto puede ocurrir si el destino cierra la conexión antes de que se agote el tiempo de inactividad o si el cliente envía una solicitud con el formato incorrecto.
elb_status_code	Código de estado de la respuesta desde el equilibrador de carga.
target_status_code	Código de estado de la respuesta desde el destino. Este valor se registra únicamente si se estableció una conexión con el destino y este envió una respuesta. De lo contrario, se establece en -.
received_bytes	Tamaño de la solicitud, en bytes, recibida desde el cliente (solicitante). Para las solicitudes HTTP, incluye los encabezados. Pues WebSockets, este es el número total de bytes recibidos del cliente en la conexión.
sent_bytes	Tamaño de la respuesta, en bytes, enviada al cliente (solicitante). Para las solicitudes HTTP, incluye los encabezados. Pues WebSockets, es el número total de bytes enviados al cliente en la conexión.
"request"	La línea de solicitud del cliente entre comillas y registrada con el siguiente formato: Método HTTP + protocolo://host:puerto/uri + versión de HTTP. El equilibrador de carga conserva la URL que envía el cliente, tal como está, al registrar el URI de la solicitud. No establece el tipo de contenido para el archivo de registro de acceso. Al procesar este campo, tenga en cuenta cómo envió el cliente la URL.
"user_agent"	Cadena User-Agent que identifica el cliente que originó la solicitud, entre comillas. La cadena consta de uno o varios identificadores de producto, con el formato producto[/versión]. Si la cadena tiene más de 8 KB, se trunca.

Campo	Descripción
ssl_cipher	[Agente de escucha HTTPS] Cifrado SSL. Este valor se establece en - si el oyente no es un oyente HTTPS.
ssl_protocol	[Agente de escucha HTTPS] El protocolo SSL. Este valor se establece en - si el oyente no es un oyente HTTPS.
target_group_arn	Nombre de recurso de Amazon (ARN) del grupo de destino.
"trace_id"	El contenido del encabezado X-Amzn-Trace-Id, entre comillas.
"domain_name"	[Agente de escucha HTTPS] El dominio de SNI proporcionado por el cliente durante el protocolo de TLS, entre comillas. Este valor está establecido en - si el cliente no admite SNI o el dominio no coincide con un certificado y se presenta al cliente el certificado predeterminado.
"chosen_cert_arn"	[Agente de escucha HTTPS] El ARN del certificado presentado al cliente, entre comillas. Este valor se establece en `session-reused` si se reutiliza la sesión. Este valor se establece en - si el oyente no es un oyente HTTPS.
matched_rule_priority	El valor de prioridad de la regla que coincide con la solicitud. Si hay una regla que coincide, este es un valor de 1 a 50 000. Si no hay ninguna regla que coincida, y se ha realizado la acción predeterminada, este valor se establece en 0. Si se produce un error durante la evaluación de reglas, se establece en -1. Para cualquier otro error, se establece en -.
request_creation_time	Hora a la que el equilibrador de carga recibió la solicitud del cliente, en formato ISO 8601.
"actions_executed"	Las acciones realizadas al procesar la solicitud, entre comillas. Este valor es una lista separada por comas que puede incluir los valores que se describen en Medidas tomadas. Si no se ha realizado ninguna acción, como en el caso de una solicitud con formato incorrecto, este valor se establece en -.

Campo	Descripción
"redirect_url"	URL del destino de redirección incluida en el encabezado de ubicación de la respuesta HTTP entre comillas dobles. Si no se ejecutan acciones de redirección, este valor se establece en -.
"error_reason"	El código de motivo de error, entre comillas dobles. Si la solicitud produjo un error, este es uno de los códigos de error que se describen en Códigos de motivo de error. Si las acciones realizadas no incluyen una acción de autenticación o el destino no es una función de Lambda, este valor se establece en -.
"target:port_list"	Una lista delimitada por espacios de direcciones IP y puertos para los destinos que procesaron esta solicitud, entre comillas dobles. Actualmente, esta lista puede contener un elemento y coincide con el campo target:port. Si el cliente no envió una solicitud completa, el equilibrador de carga no puede enviar la solicitud a un destino, en cuyo caso este valor se establece en -. Si el destino es una función de Lambda, este valor se establece en -. Si la solicitud está bloqueada por AWS WAF, este valor se establece en - y el valor de elb_status_code se establece en 403.
"target_status_code_list"	Una lista delimitada por espacios de códigos de estado de las respuestas de los destinos, entre comillas dobles. Actualmente, esta lista puede contener un elemento y coincide con el campo target_status_code. Este valor se registra únicamente si se estableció una conexión con el destino y este envió una respuesta. De lo contrario, se establece en -.
"classification"	La clasificación de la mitigación de la desincronización, entre comillas dobles. Si la solicitud no cumple con RFC 7230, los valores posibles son Aceptable, Ambiguo y Grave. Si la solicitud cumple con RFC 7230, este valor se establece en -.

Campo	Descripción
"classification_reason"	El código de motivo de la clasificación, entre comillas dobles. Si la solicitud no cumple con la RFC 7230, se trata de uno de los códigos de clasificación descritos en Motivos de la clasificación. Si la solicitud cumple con RFC 7230, este valor se establece en -.
conn_trace_id	El identificador de trazabilidad de la conexión es un identificador opaco único que se utiliza para identificar cada conexión. Una vez establecida una conexión con un cliente, las solicitudes posteriores de este cliente incluirán este ID en sus respectivas entradas del registro de acceso. Este ID actúa como una clave externa para crear un enlace entre los registros de conexión y acceso.

Medidas tomadas

El equilibrador de carga almacena las acciones que realiza en el campo actions_executed del registro de acceso.

- `authenticate`: el equilibrador de carga validó la sesión, autenticó al usuario y agregó la información del usuario a los encabezados de las solicitudes, según lo especificado en la configuración de la regla.
- `fixed-response`: el equilibrador de carga emitió una respuesta fija, según lo especificado en la configuración de la regla.
- `forward`: el equilibrador de carga reenvió la solicitud a un destino, según lo especificado en la configuración de la regla.
- `redirect`: el equilibrador de carga redirigió la solicitud a otra URL, según lo especificado en la configuración de la regla.
- `waf`: el equilibrador de carga reenvió la solicitud a AWS WAF para determinar si debía reenviarse al destino. Si esta es la acción final, AWS WAF determinó que la solicitud debe rechazarse.
- `waf-failed`— El balanceador de cargas intentó reenviar la solicitud AWS WAF, pero el proceso falló.

Motivos de la clasificación

Si una solicitud no cumple con RFC 7230, el equilibrador de carga almacena uno de los siguientes códigos en el campo classification_reason del registro de acceso. Para obtener más información, consulte Modo de mitigación de desincronización.

Código	Descripción	Clasificación
`AmbiguousUri`	El URI de la solicitud contiene caracteres de control.	Ambigua
`BadContentLength`	El encabezado Content-Length contiene un valor que no se puede analizar o que no es un número válido.	Grave
`BadHeader`	Un encabezado contiene un carácter nulo o un retorno de carro.	Grave
`BadTransferEncoding`	El encabezado Transfer-Encoding contiene un valor incorrecto.	Grave
`BadUri`	El URI de la solicitud contiene un carácter nulo o un retorno de carro.	Grave
`BadMethod`	El método de la solicitud tiene un formato incorrecto.	Grave
`BadVersion`	La versión de la solicitud tiene un formato incorrecto.	Grave
`BothTeClPresent`	La solicitud contiene un encabezado Transfer-Encoding y un encabezado Content-Length.	Ambigua
`DuplicateContentLength`	Hay varios encabezados Content-Length con el mismo valor.	Ambigua
`EmptyHeader`	Un encabezado está vacío o hay una línea que solo contiene espacios.	Ambigua

Código	Descripción	Clasificación
`GetHeadZeroContentLength`	Hay un encabezado Content-Length con un valor de 0 para una solicitud GET o HEAD.	Aceptable
`MultipleContentLength`	Hay varios encabezados Content-Length con valores diferentes.	Grave
`MultipleTransferEncodingChunked`	Hay varios encabezados Transfer-Encoding fragmentados.	Grave
`NonCompliantHeader`	Un encabezado contiene un carácter de control o no ASCII.	Aceptable
`NonCompliantVersion`	La versión de la solicitud contiene un valor incorrecto.	Aceptable
`SpaceInUri`	El URI de la solicitud contiene un espacio sin codificación URL.	Aceptable
`SuspiciousHeader`	Hay un encabezado que se puede normalizar a Transfer-Encoding o Content-Length mediante técnicas comunes de normalización de texto.	Ambigua
`UndefinedContentLengthSemantics`	Hay un encabezado Content-Length definido para una solicitud GET o HEAD.	Ambigua
`UndefinedTransferEncodingSemantics`	Hay un encabezado Transfer-Encoding definido para una solicitud GET o HEAD.	Ambigua

Códigos de motivo de error

Si el equilibrador de carga no puede completar una acción de autenticación, el equilibrador de carga almacena uno de los siguientes códigos de motivo de error en el campo error_reason del registro de acceso. El balanceador de cargas también incrementa la métrica correspondiente. CloudWatch Para obtener más información, consulte Autenticación de usuarios mediante un Equilibrador de carga de aplicación.

Código	Descripción	Métrica
`AuthInvalidCookie`	La cookie de autenticación no es válida.	`ELBAuthFailure`
`AuthInvalidGrantError`	El código de concesión de autorización del punto de conexión del token no es válido.	`ELBAuthFailure`
`AuthInvalidIdToken`	El token de ID no es válido.	`ELBAuthFailure`
`AuthInvalidStateParam`	El parámetro de estado no es válido.	`ELBAuthFailure`
`AuthInvalidTokenResponse`	La respuesta desde el punto de conexión del token no es válida.	`ELBAuthFailure`
`AuthInvalidUserinfoResponse`	La respuesta desde el punto de conexión de información de usuario no es válida.	`ELBAuthFailure`
`AuthMissingCodeParam`	En la respuesta de autenticación desde el punto de conexión de autorización falta un parámetro de consulta denominado ‘code’.	`ELBAuthFailure`
`AuthMissingHostHeader`	En la respuesta de autenticación desde el punto de conexión de autorización falta un campo de encabezado de host.	`ELBAuthError`

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

Si se produce un error en una solicitud a un grupo de destino ponderado, el equilibrador de carga almacena uno de los siguientes códigos de error en el campo error_reason del registro de acceso.

Código	Descripción
`AWSALBTGCookieInvalid`	La AWSALBTG cookie, que se utiliza con los grupos objetivo ponderados, no es válida. Por ejemplo, el equilibrador de carga

Código	Descripción
	devuelve este error cuando los valores de la cookie están codificados como URL.
`WeightedTargetGroupsUnhandledException`	El equilibrador de carga encontró una excepción no administrada.

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

Código	Descripción	Métrica
`LambdaAccessDenied`	El equilibrador de carga no tenía permiso para invocar la función de Lambda.	`LambdaUserError`
`LambdaBadRequest`	Se ha producido un error en la invocación lambda porque los encabezados o el cuerpo de la solicitud del cliente no contenían únicamente caracteres UTF-8.	`LambdaUserError`
`LambdaConnectionError`	El equilibrador de carga no puede conectarse a Lambda.	`LambdaInternalError`
`LambdaConnectionTimeout`	Se agotó el tiempo de espera al intentar conectarse a Lambda.	`LambdaInternalError`
`LambdaEC2AccessDeniedException`	Amazon EC2 denegó el acceso a Lambda durante la inicialización de la función.	`LambdaUserError`
`LambdaEC2ThrottledException`	Amazon EC2 aplicó una restricción a Lambda durante la inicialización de la función.	`LambdaUserError`

Código	Descripción	Métrica
`LambdaEC2UnexpectedException`	Amazon EC2 detectó una excepción inesperada durante la inicialización de la función.	`LambdaUserError`
`LambdaENILimitReachedException`	Lambda no pudo crear una interfaz de red en la VPC especificada en la configuración de la función de Lambda porque se superó el límite de interfaces de red.	`LambdaUserError`
`LambdaInvalidResponse`	La respuesta de la función de Lambda no tiene el formato correcto o no incluye campos obligatorios.	`LambdaUserError`
`LambdaInvalidRuntimeException`	La versión especificada del tiempo de ejecución de Lambda no se admite.	`LambdaUserError`
`LambdaInvalidSecurityGroupIDException`	El ID de grupo de seguridad especificado en la configuración de la función de Lambda no es válido.	`LambdaUserError`
`LambdaInvalidSubnetIDException`	El ID de subred especificado en la configuración de la función de Lambda no es válido.	`LambdaUserError`
`LambdaInvalidZipFileException`	Lambda no pudo descomprimir el archivo zip de la función especificada.	`LambdaUserError`
`LambdaKMSAccessDeniedException`	Lambda no pudo descifrar las variables de entorno porque se denegó el acceso a la clave de KMS. Compruebe los permisos de KMS de la función de Lambda.	`LambdaUserError`

Código	Descripción	Métrica
`LambdaKMSDisabledException`	Lambda no pudo descifrar las variables de entorno, porque se deshabilitó la clave de KMS especificada. Compruebe la configuración de la clave de KMS de la función de Lambda.	`LambdaUserError`
`LambdaKMSInvalidStateException`	Lambda no pudo descifrar las variables de entorno porque el estado de la clave de KMS no era válido. Compruebe la configuración de la clave de KMS de la función de Lambda.	`LambdaUserError`
`LambdaKMSNotFoundException`	Lambda no pudo descifrar las variables de entorno porque no se encontró la clave de KMS. Compruebe la configuración de la clave de KMS de la función de Lambda.	`LambdaUserError`
`LambdaRequestTooLarge`	El tamaño del cuerpo de la solicitud era superior a 1 MB.	`LambdaUserError`
`LambdaResourceNotFound`	No se pudo encontrar la función de Lambda.	`LambdaUserError`
`LambdaResponseTooLarge`	El tamaño de la respuesta era superior a 1 MB.	`LambdaUserError`
`LambdaServiceException`	Lambda detectó un error interno.	`LambdaInternalError`
`LambdaSubnetIPAddressLimitReachedException`	Lambda no pudo configurar el acceso a la VPC de la función de Lambda porque una o varias subredes no tenían direcciones IP disponibles.	`LambdaUserError`
`LambdaThrottling`	La función de Lambda se rechazó porque había demasiadas solicitudes.	`LambdaUserError`

Código	Descripción	Métrica
`LambdaUnhandled`	La función de Lambda encontró una excepción no administrada.	`LambdaUserError`
`LambdaUnhandledException`	El equilibrador de carga encontró una excepción no administrada.	`LambdaInternalError`
`LambdaWebsocketNotSupported`	WebSockets Lambda no los admite.	`LambdaUserError`

Si el balanceador de cargas detecta un error al reenviar las solicitudes AWS WAF, almacena uno de los siguientes códigos de error en el campo error_reason del registro de acceso.

Código	Descripción
`WAFConnectionError`	El balanceador de cargas no se puede conectar a. AWS WAF
`WAFConnectionTimeout`	Se agotó el AWS WAF tiempo de espera de la conexión.
`WAFResponseReadTimeout`	Se ha agotado el AWS WAF tiempo de espera de una solicitud.
`WAFServiceError`	AWS WAF devolvió un error de 5XX.
`WAFUnhandledException`	El equilibrador de carga encontró una excepción no administrada.

Ejemplo de entradas de registro

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

Ejemplo de entrada HTTP

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

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

Ejemplo de entrada HTTPS

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

```
https 2018-07-02T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 10.0.0.1:80 0.086 0.048 0.037 200 200 0 57
"GET https://www.example.com:443/ HTTP/1.1" "curl/7.46.0" ECDHE-RSA-AES128-GCM-SHA256
 TLSv1.2
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337281-1d84f3d73c47ec4e58577259" "www.example.com" "arn:aws:acm:us-
east-2:123456789012:certificate/12345678-1234-1234-1234-123456789012"
1 2018-07-02T22:22:48.364000Z "authenticate,forward" "-" "-" "10.0.0.1:80" "200" "-"
 "-" TID_123456
```

Ejemplo de entrada HTTP/2

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

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

Ejemplo WebSockets de entrada

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

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

Ejemplo de WebSockets entrada segura

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

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

Entradas de ejemplo de funciones de Lambda

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

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

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

```
http 2018-11-30T22:23:00.186641Z app/my-loadbalancer/50dc6c495c0c9188
192.168.131.39:2817 - 0.000 0.001 0.000 502 - 34 366
```

```
"GET http://www.example.com:80/ HTTP/1.1" "curl/7.46.0" - -
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067
"Root=1-58337364-23a8c76965a2ef7629b185e3" "-" "-"
0 2018-11-30T22:22:48.364000Z "forward" "-" "LambdaInvalidResponse" "-" "-" "-" "-"
```

Procesamiento de archivos de registro de acceso

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

Si existe una gran cantidad de demanda en el sitio web, el equilibrador de carga puede generar archivos registro con gigabytes de datos. Es posible que no pueda procesar una cantidad tan grande de datos mediante el line-by-line procesamiento. En tal caso, podría ser preciso utilizar herramientas de análisis que ofrezcan soluciones de procesamiento en paralelo. Por ejemplo, puede utilizar las siguientes herramientas de análisis para analizar y procesar los registros de acceso:

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

Registros de acceso del Equilibrador de carga de aplicación

Al habilitar los registros de acceso del equilibrador de carga, debe especificar el nombre del bucket de S3 donde el equilibrador de carga almacenará los registros. El bucket debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir en el bucket.

Tareas

- Paso 1: Crear un bucket de S3
- Paso 2: Adjuntar una política al bucket de S3
- Paso 3: configurar los registros de acceso
- Paso 4: verificar los permisos del bucket

- Resolución de problemas

Paso 1: Crear un bucket de S3

Al habilitar los registros de acceso, es preciso especificar un bucket de S3 para estos. Puede utilizar un bucket existente o crear uno específico para los registros de acceso. El bucket debe cumplir los siguientes requisitos.

Requisitos

- El bucket debe estar ubicado en la misma región que el equilibrador de carga. El bucket y el equilibrador de carga pueden ser propiedad de diferentes cuentas.
- La única opción de cifrado del lado del servidor que se admite son claves administradas por Amazon S3 (SSE-S3). Para obtener más información, consulte Claves de cifrado administradas por Amazon S3 (SSE-S3).

Para crear un bucket de S3 con la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija Crear bucket.
3. En la página Create bucket (Crear un bucket), realice las siguientes acciones:
    a. En Nombre del bucket, escriba un nombre para el bucket. Este nombre debe ser único entre todos los nombres de buckets de Amazon S3. En algunas regiones, es posible que haya restricciones adicionales para los nombres de los buckets. Para obtener más información, consulte Restricciones y limitaciones de los buckets en la Guía del usuario de Amazon Simple Storage Service.
    b. En AWS Region (Región de), seleccione la región donde ha creado el equilibrador de carga.
    c. Para el cifrado predeterminado, elija las claves administradas por Amazon S3 (SSE-S3).
    d. Elija Crear bucket.

Paso 2: Adjuntar una política al bucket de S3

El bucket de S3 debe tener una política que conceda permiso a Elastic Load Balancing para escribir los registros de acceso en el bucket. Las políticas de bucket son colecciones de instrucciones JSON

escritas en el lenguaje de la política de acceso para definir los permisos de acceso al bucket. Cada instrucción incluye información sobre un único permiso y contiene una serie de elementos.

Si utiliza un bucket existente que ya tiene una política adjunta, puede agregar la instrucción para los registros de acceso de Elastic Load Balancing a la política. En este caso, recomendamos evaluar el conjunto de permisos resultante para asegurarse de que sean adecuados para los usuarios que necesitan obtener acceso al bucket en relación con los registros de acceso.

Políticas de bucket disponibles

La política de bucket que utilice dependerá de la zona y del tipo de zona. Región de AWS

Regiones disponibles a partir de agosto de 2022 en adelante

Esta política otorga permisos al servicio de entrega de registros especificado. Utilice esta política para los equilibradores de carga en las zonas de disponibilidad y las zonas locales de las siguientes regiones:

- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Melbourne)
- Oeste de Canadá (Calgary)
- Europa (España)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (EAU)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*"
    }
  ]
```

```
}
```

Regiones disponibles antes de agosto de 2022

Esta política concede permisos al ID de cuenta de Elastic Load Balancing especificado. Utilice esta política para los equilibradores de carga de las zonas de disponibilidad o las zonas locales de las regiones de en la siguiente lista.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*"
    }
  ]
}
```

Sustituya *elb-account-id* por el ID de Elastic Cuenta de AWS Load Balancing de su región:

- 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

Sustituya *my-s3-arn* por el ARN de la ubicación de sus registros de acceso. El ARN que especifique dependerá de si planea especificar un prefijo al habilitar los registros de acceso en el paso 3.

- Ejemplo de ARN con un prefijo

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

- Ejemplo de ARN sin un prefijo

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

Usar when is. NotPrincipalEffectDeny

Si la política de bucket de Amazon S3 utiliza `Effect` el valor `Deny` e incluye `NotPrincipal` lo que se muestra en el siguiente ejemplo, asegúrese de que `logdelivery.elasticloadbalancing.amazonaws.com` esté incluido en la `Service` lista.

```
{
  "Effect": "Deny",
  "NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
    ]
```

```
  }
},
```

AWS GovCloud (US) Regions

Esta política concede permisos al ID de cuenta de Elastic Load Balancing especificado. Usa esta política para los balanceadores de carga en las Zonas de Disponibilidad o en las Zonas Locales de las AWS GovCloud (US) regiones de la lista siguiente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "my-s3-arn"
    }
  ]
}
```

Sustituya *elb-account-id* por el ID de Elastic Cuenta de AWS Load Balancing de su región: AWS GovCloud (US)

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

Sustituya *my-s3-arn* por el ARN de la ubicación de sus registros de acceso. El ARN que especifique dependerá de si planea especificar un prefijo al habilitar los registros de acceso en el paso 3.

- Ejemplo de ARN con un prefijo

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

- Ejemplo de ARN sin un prefijo

```
arn:aws-us-gov:s3:::bucket-name/AWSLogs/aws-account-id/*
```

Zonas Outposts

La siguiente política otorga permisos al servicio de entrega de registros especificado. Utilice esta política para los equilibradores de carga en las zonas Outposts.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "logdelivery.elb.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/your-aws-account-id/*",
    "Condition": {
        "StringEquals": {
            "s3:x-amz-acl": "bucket-owner-full-control"
        }
    }
}
```

Para adjuntar una política de bucket para los registros de acceso a su bucket con la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Seleccione el nombre del bucket para abrir la página de detalles.
3. Elija Permisos y, a continuación, seleccione Política de bucket, Editar.
4. Actualice la política de bucket para conceder los permisos necesarios.
5. Elija Guardar cambios.

Paso 3: configurar los registros de acceso

Utilice el siguiente procedimiento para configurar los registros de acceso a fin de capturar y entregar los archivos de registro al bucket de S3.

Requisitos

El bucket debe cumplir los requisitos descritos en el paso 1 y debe adjuntar una política de bucket tal como se describe en el paso 2. Si especifica un prefijo, no debe incluir la cadena "». AWSLogs

Para habilitar los registros de acceso para el equilibrador de carga desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Para la Monitorización, active los registros de acceso.
6. En URI de S3, ingrese el URI de S3 correspondiente a los archivos de registro. El URI que especifique depende de si utiliza un prefijo.
   - URI con un prefijo: `s3://bucket-name/prefix`
   - URI sin un prefijo: `s3://bucket-name`
7. Elija Guardar cambios.

Para habilitar los registros de acceso mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes.

Para administrar el bucket de S3 para los registros de acceso

Asegúrese de deshabilitar los registros de acceso antes de eliminar el bucket que configuró para los registros de acceso. De lo contrario, si existe un nuevo bucket con el mismo nombre y la política de bucket requerida pero creada en una Cuenta de AWS que no le pertenece, Elastic Load Balancing podría escribir los registros de acceso del equilibrador de carga en este nuevo bucket.

Paso 4: verificar los permisos del bucket

Después de habilitar los registros de acceso para el equilibrador de carga, Elastic Load Balancing valida el bucket de S3 y crea un archivo de prueba para garantizar que la política del bucket especifica los permisos necesarios. Puede utilizar la consola de Amazon S3 para comprobar que se ha creado el archivo de prueba. El archivo de prueba no es un archivo de registro de acceso real; no contiene registros de ejemplo.

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

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Seleccione el nombre del bucket que especificó para los registros de acceso.

3. Vaya al archivo registro de prueba, `ELBAccessLogTestFile`. La ubicación depende de si utiliza un prefijo.

   - Ubicación con un prefijo: *my-bucket*/*prefix*/AWSLogs/*123456789012*/ELBAccessLogTestFile
   - Ubicación sin un prefijo: *my-bucket*/AWSLogs/*123456789012*/ELBAccessLogTestFile

Resolución de problemas

Si recibe un error de acceso denegado, estas pueden ser causas posibles:

- La política del bucket no concede permiso a Elastic Load Balancing para escribir registros de acceso en el bucket. Compruebe que está utilizando la política de bucket correcta para la región. Compruebe que el ARN del recurso utilice el mismo nombre de bucket que especificó al habilitar los registros de acceso. Compruebe que el ARN del recurso no incluya un prefijo si no especificó un prefijo al habilitar los registros de acceso.
- El bucket usa una opción de cifrado del lado del servidor no compatible. El bucket debe usar claves administradas por Amazon S3 (SSE-S3).

Registros de acceso deshabilitados del Equilibrador de carga de aplicación

Se íedem deshabilitar los registros de acceso del equilibrador de carga en cualquier momento. Después de deshabilitar los registros de acceso, los registros de acceso permanecerán en el bucket de S3 hasta que los elimine. Para obtener más información, consulte Trabajar con buckets en la Guía del usuario de Amazon Simple Storage Service.

Desactivar el registro de acceso desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Para la Monitorización, desactive los registros de acceso.
6. Elija Guardar cambios.

Para deshabilitar los registros de acceso mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes.

Registros de conexión para su Application Load Balancer

Elastic Load Balancing proporciona registros de conexión que capturan información detallada sobre las solicitudes enviadas al balanceador de carga. Cada registro contiene información como la dirección IP y el puerto del cliente, el puerto de escucha, el protocolo y el cifrado TLS utilizados, la latencia del protocolo de enlace TLS, el estado de la conexión y los detalles del certificado del cliente. Puede usar estos registros de conexión para analizar los patrones de solicitudes y solucionar problemas.

Los registros de conexiones son una función opcional de Elastic Load Balancing que está deshabilitada de forma predeterminada. Tras habilitar los registros de conexión para el balanceador de carga, Elastic Load Balancing captura los registros y los almacena en el bucket de Amazon S3 que especifique, como archivos comprimidos. Puede deshabilitar los registros de conexión en cualquier momento.

Se cobran los costos de almacenamiento en Amazon S3, pero no el ancho de banda que Elastic Load Balancing utilice para enviar los archivos de registros a Amazon S3. Para obtener más información acerca de los costos de almacenamiento, consulte Precios de Amazon S3.

Contenido

- Archivos de registro de conexiones
- Entradas de registro de conexión
- Ejemplo de entradas de registro
- Procesamiento de archivos de registro de conexiones
- Habilite los registros de conexión para su Application Load Balancer
- Inhabilite los registros de conexión para su Application Load Balancer

Archivos de registro de conexiones

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

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

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

bucket

Nombre del bucket de S3.

prefix

(Opcional) El prefijo (jerarquía lógica) del bucket. El prefijo que especifique no debe incluir la cadena `AWSLogs`. Para obtener más información, consulte Organizar objetos con prefijos.

`AWSLogs`

Agregamos la parte del nombre de archivo que comienza por `AWSLogs` después del nombre del bucket y el prefijo que especifique.

aws-account-id

El ID de AWS cuenta del propietario.

region

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

aaaa/mm/dd

La fecha de entrega del log.

load-balancer-id

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

end-time

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

ip-address

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

random-string

Una cadena generada aleatoriamente por el sistema.

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

```
s3://my-bucket/my-prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2022/05/01/conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

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

```
s3://my-bucket/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2022/05/01/conn_log.123456789012_elasticloadbalancing_us-east-2_app.my-
loadbalancer.1234567890abcdef_20220215T2340Z_172.160.001.192_20sg8hgm.log.gz
```

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

Entradas de registro de conexión

Cada intento de conexión tiene una entrada en un archivo de registro de conexiones. La forma en que se envían las solicitudes de los clientes depende de si la conexión es persistente o no persistente. Las conexiones no persistentes tienen una sola solicitud, lo que crea una entrada única en el registro de acceso y en el registro de conexiones. Las conexiones persistentes tienen varias solicitudes, lo que crea varias entradas en el registro de acceso y una sola entrada en el registro de conexiones.

Contenido

- Sintaxis
- Códigos de motivo de error

Sintaxis

Las entradas del registro de conexiones utilizan el siguiente formato:

```
[timestamp] [client_ip] [client_port] [listener_port] [tls_protocol] [tls_cipher]
 [tls_handshake_latency] [leaf_client_cert_subject] [leaf_client_cert_validity]
 [leaf_client_cert_serial_number] [tls_verify_status]
```

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

Campo	Descripción
Marca de tiempo	La hora, en formato ISO 8601, en la que el balanceador de carga estableció correctamente o no pudo establecer una conexión.
client_ip	Dirección IP del cliente solicitante.
client_port	El puerto del cliente solicitante.
listener_port	El puerto del agente de escucha del balanceador de cargas que recibe la solicitud del cliente.
tls_protocol	[Listener HTTPS] El protocolo SSL/TLS utilizado durante los apretones de manos. Este campo está configurado para solicitudes que no son de SSL/TLS. -
tls_cipher	[Listener HTTPS] El protocolo SSL/TLS utilizado durante los apretones de manos. Este campo está configurado para solicitudes que no son de SSL/TLS. -
tls_handshake_latency	[Listener HTTPS] El tiempo total en segundos, con una precisión de milisegundos, transcurrido hasta que se estableció un apretón de manos exitoso. Este campo se establece en los siguientes casos: - • La solicitud entrante no es una solicitud de SSL/TLS. • El apretón de manos no se ha establecido correctamente.
leaf_client_cert_subject	[Listener HTTPS] El nombre del asunto del certificado de cliente Leaf. Este campo se establece en los siguientes - casos:

Campo	Descripción
	• La solicitud entrante no es una solicitud de SSL/TLS. • El agente de escucha del balanceador de cargas no está configurado con mTLS activado. • El servidor no puede cargar ni analizar el certificado del cliente Leaf.
leaf_client_cert_valid	[HTTPS listener] La validez, con `not-before` y `not-after` en formato ISO 8601, del certificado de cliente Leaf. Este campo se establece en los siguientes casos: - • La solicitud entrante no es una solicitud de SSL/TLS. • El agente de escucha del balanceador de cargas no está configurado con mTLS activado. • El servidor no puede cargar/analizar el certificado del cliente Leaf.
leaf_client_cert_serial_number	[Listener HTTPS] El número de serie del certificado de cliente Leaf. Este campo se establece en los siguientes - casos: • La solicitud entrante no es una solicitud de SSL/TLS. • El agente de escucha del balanceador de cargas no está configurado con mTLS activado. • El servidor no puede cargar/analizar el certificado del cliente Leaf.
tls_verify_status	[Listener HTTPS] El estado de la solicitud de conexión. Este valor corresponde a `Success` si la conexión se estableció correctamente. En una conexión fallida, el valor es`Failed:$error_code` .
conn_trace_id	El identificador de trazabilidad de la conexión es un identificador opaco único que se utiliza para identificar cada conexión. Una vez establecida una conexión con un cliente, las solicitudes posteriores de este cliente incluirán este ID en sus respectivas entradas del registro de acceso. Este ID actúa como una clave externa para crear un enlace entre los registros de conexión y acceso.

Códigos de motivo de error

Si el balanceador de cargas no puede establecer una conexión, guarda uno de los siguientes códigos de motivo en el registro de conexiones.

Código	Descripción	
`ClientCertMaxChainDepthExceeded`	Se ha superado la profundidad máxima de la cadena de certificados de cliente	
`ClientCertMaxSizeExceeded`	Se ha superado el tamaño máximo del certificado de cliente	
`ClientCertCrlHit`	La CA ha revocado el certificado de cliente	
`ClientCertCrlProcessingError`	Error al procesar la CRL	
`ClientCertUntrusted`	El certificado del cliente no es de confianza	
`ClientCertNotYetValid`	El certificado de cliente aún no es válido	
`ClientCertExpired`	El certificado de cliente ha caducado	
`ClientCertTypeUnsupported`	El tipo de certificado de cliente no es compatible	
`ClientCertInvalid`	El certificado de cliente no es válido	

Código	Descripción	
`ClientCertRejected`	El certificado de cliente se rechaza mediante una validación de servidor personalizada	
`UnmappedConnectionError`	Error de conexión en tiempo de ejecución no mapeado	

Ejemplo de entradas de registro

A continuación se muestran ejemplos de entradas del registro de conexiones.

A continuación se muestra un ejemplo de entrada de registro para una conexión correcta con un agente de escucha HTTPS con el modo de verificación TLS mutua activado en el puerto 443:

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-GCM-
SHA256 4.036 "CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z FEF257372D5C14D4 Success
```

El siguiente es un ejemplo de entrada de registro para una conexión fallida con un agente de escucha HTTPS con el modo de verificación TLS mutua habilitado en el puerto 443. :

```
2023-10-04T17:05:15.514108Z 203.0.113.1 36280 443 TLSv1.2 ECDHE-RSA-AES128-
GCM-SHA256 - "CN=amazondomains.com,O=endEntity,L=Seattle,ST=Washington,C=US"
 NotBefore=2023-09-21T22:43:21Z;NotAfter=2026-06-17T22:43:21Z FEF257372D5C14D4
 Failed:ClientCertUntrusted
```

Procesamiento de archivos de registro de conexiones

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

Si existe una gran cantidad de demanda en el sitio web, el equilibrador de carga puede generar archivos registro con gigabytes de datos. Es posible que no pueda procesar una cantidad tan grande de datos mediante 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 analíticas para analizar y procesar los registros de conexiones:

- Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar.
- Loggly
- Splunk
- Sumo Logic

Habilite los registros de conexión para su Application Load Balancer

Al habilitar los registros de conexión para el balanceador de cargas, debes especificar el nombre del depósito de S3 en el que el balanceador de cargas almacenará los registros. El bucket debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir en el bucket.

Tareas

- Paso 1: Crear un bucket de S3
- Paso 2: Adjuntar una política al bucket de S3
- Paso 3: Configurar los registros de conexión
- Paso 4: verificar los permisos del bucket
- Resolución de problemas

Paso 1: Crear un bucket de S3

Al habilitar los registros de conexión, debe especificar un bucket de S3 para los registros de conexión. Puede usar un depósito existente o crear uno específico para los registros de conexión. El bucket debe cumplir los siguientes requisitos.

Requisitos

- El bucket debe estar ubicado en la misma región que el equilibrador de carga. El bucket y el equilibrador de carga pueden ser propiedad de diferentes cuentas.
- La única opción de cifrado del lado del servidor que se admite son claves administradas por Amazon S3 (SSE-S3). Para obtener más información, consulte Claves de cifrado administradas por Amazon S3 (SSE-S3).

Para crear un bucket de S3 con la consola de Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.

2. Elija Crear bucket.
3. En la página Create bucket (Crear un bucket), realice las siguientes acciones:

    a. En Nombre del bucket, escriba un nombre para el bucket. Este nombre debe ser único entre todos los nombres de buckets de Amazon S3. En algunas regiones, es posible que haya restricciones adicionales para los nombres de los buckets. Para obtener más información, consulte Restricciones y limitaciones de los buckets en la Guía del usuario de Amazon Simple Storage Service.
    b. En AWS Region (Región de), seleccione la región donde ha creado el equilibrador de carga.
    c. Para el cifrado predeterminado, elija las claves administradas por Amazon S3 (SSE-S3).
    d. Elija Crear bucket.

Paso 2: Adjuntar una política al bucket de S3

El bucket de S3 debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir los registros de conexión en el bucket. Las políticas de bucket son colecciones de instrucciones JSON escritas en el lenguaje de la política de acceso para definir los permisos de acceso al bucket. Cada instrucción incluye información sobre un único permiso y contiene una serie de elementos.

Si utilizas un bucket existente que ya tiene una política adjunta, puedes añadir la declaración para los registros de conexión de Elastic Load Balancing a la política. Si lo hace, le recomendamos que evalúe el conjunto de permisos resultante para asegurarse de que son adecuados para los usuarios que necesitan acceder al depósito para los registros de conexión.

Políticas de bucket disponibles

La política de bucket que utilices depende de la zona Región de AWS y del tipo de zona.

Regiones disponibles a partir de agosto de 2022 en adelante

Esta política otorga permisos al servicio de entrega de registros especificado. Utilice esta política para los equilibradores de carga en las zonas de disponibilidad y las zonas locales de las siguientes regiones:

- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Melbourne)

- Europa (España)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (EAU)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*"
    }
  ]
}
```

Regiones disponibles antes de agosto de 2022

Esta política concede permisos al ID de cuenta de Elastic Load Balancing especificado. Utilice esta política para los equilibradores de carga de las zonas de disponibilidad o las zonas locales de las regiones de en la siguiente lista.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
       "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*"
    }
  ]
}
```

Sustituya *elb-account-id* por el ID de Elastic Cuenta de AWS Load Balancing de su región:

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

Sustituya *my-s3-arn* por el ARN de la ubicación de los registros de conexión. El ARN que especifique depende de si planea especificar un prefijo al habilitar los registros de conexión en el paso 3.

- Ejemplo de ARN con un prefijo

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

- Ejemplo de ARN sin un prefijo

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

Usar **`NotPrincipal`** cuándo **`Effect`** es. **`Deny`**

Si la política de bucket de Amazon S3 utiliza `Effect` el valor `Deny` e incluye `NotPrincipal` lo que se muestra en el siguiente ejemplo, asegúrese de que `logdelivery.elasticloadbalancing.amazonaws.com` esté incluido en la `Service` lista.

```
{
"Effect": "Deny",
"NotPrincipal": {
    "Service": [
       "logdelivery.elasticloadbalancing.amazonaws.com",
       "example.com"
},
```

Para adjuntar una política de bucket para los registros de conexión a su bucket mediante la consola Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Seleccione el nombre del bucket para abrir la página de detalles.
3. Elija Permisos y, a continuación, seleccione Política de bucket, Editar.
4. Actualice la política de bucket para conceder los permisos necesarios.
5. Elija Guardar cambios.

Paso 3: Configurar los registros de conexión

Utilice el siguiente procedimiento para configurar los registros de conexión a fin de capturar y entregar los archivos de registro a su bucket de S3.

Requisitos

El bucket debe cumplir los requisitos descritos en el paso 1 y debe adjuntar una política de bucket tal como se describe en el paso 2. Si especifica un prefijo, no debe incluir la cadena "AWSLogs».

Para habilitar los registros de conexión de tu balanceador de cargas mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Para la supervisión, activa los registros de conexión.
6. En URI de S3, ingrese el URI de S3 correspondiente a los archivos de registro. El URI que especifique depende de si utiliza un prefijo.
   - URI con un prefijo: `s3://bucket-name/prefix`
   - URI sin un prefijo: `s3://bucket-name`
7. Elija Guardar cambios.

Para habilitar los registros de conexión mediante la AWS CLI

Utilice el comando modify-load-balancer-attributes.

Para administrar el bucket de S3 para sus registros de conexión

Asegúrese de deshabilitar los registros de conexión antes de eliminar el depósito que configuró para los registros de conexión. De lo contrario, si hay un nuevo bucket con el mismo nombre y la política de bucket requerida, pero creado en uno del Cuenta de AWS que no eres propietario, Elastic Load Balancing podría escribir los registros de conexión de tu balanceador de carga en este nuevo bucket.

Paso 4: verificar los permisos del bucket

Una vez habilitados los registros de conexión para el balanceador de cargas, Elastic Load Balancing valida el bucket S3 y crea un archivo de prueba para garantizar que la política del bucket especifique los permisos necesarios. Puede utilizar la consola de Amazon S3 para comprobar que se ha creado el archivo de prueba. El archivo de prueba no es un archivo de registro de conexiones real; no contiene registros de ejemplo.

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

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Seleccione el nombre del depósito que especificó para los registros de conexión.

3. Vaya al archivo registro de prueba, `ELBConnectionLogTestFile`. La ubicación depende de si utiliza un prefijo.

   - Ubicación con un prefijo: *my-bucket*/*prefix*/AWSLogs/*123456789012*/ELBConnectionLogTestFile
   - Ubicación sin un prefijo: *my-bucket*/AWSLogs/*123456789012*/ELBConnectionLogTestFile

Resolución de problemas

Si recibe un error de acceso denegado, estas pueden ser causas posibles:

- La política de bucket no concede permiso a Elastic Load Balancing para escribir registros de conexión en el bucket. Compruebe que está utilizando la política de bucket correcta para la región. Compruebe que el ARN del recurso utilice el mismo nombre de bucket que especificó al habilitar los registros de conexión. Compruebe que el ARN del recurso no incluya un prefijo si no lo especificó al habilitar los registros de conexión.
- El bucket usa una opción de cifrado del lado del servidor no compatible. El bucket debe usar claves administradas por Amazon S3 (SSE-S3).

Inhabilite los registros de conexión para su Application Load Balancer

Puedes deshabilitar los registros de conexión de tu balanceador de cargas en cualquier momento. Tras deshabilitar los registros de conexión, los registros de conexión permanecerán en el bucket de S3 hasta que los elimine. Para obtener más información, consulte Trabajar con buckets en la Guía del usuario de Amazon Simple Storage Service.

Para deshabilitar los registros de conexión mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Para la supervisión, desactive los registros de conexión.
6. Elija Guardar cambios.

Para deshabilitar los registros de conexión mediante la AWS CLI

Utilice el comando modify-load-balancer-attributes.

Solicite un rastreo de equilibrador de carga de aplicaciones.

Cuando el equilibrador de carga recibe una solicitud de un cliente, agrega o actualiza el encabezado X-Amzn-Trace-Id antes de enviar la solicitud al destino. Todos los servicios o aplicaciones entre el equilibrador de carga y el destino también pueden agregar o actualizar este encabezado.

Puede utilizar el rastreo de solicitudes para realizar el seguimiento de las solicitudes HTTP de los clientes a los destinos u otros servicios. Si habilita los registros de acceso, se registra el contenido del encabezado X-Amzn-Trace-Id. Para obtener más información, consulte Registros de acceso del Equilibrador de carga de aplicación.

Sintaxis

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

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

Campo

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

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

versión

Número de versión.

hora

Tiempo en formato de tiempo Unix, en segundos.

id

Identificador de rastreo.

Ejemplos

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

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

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

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

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

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

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

Limitaciones

- El equilibrador de carga actualiza el encabezado cuando recibe una solicitud entrante, no cuando recibe una respuesta.
- Si los encabezados de HTTP tienen más de 7 KB, el equilibrador de carga vuelve a escribir el encabezado X-Amzn-Trace-Id con un campo `Root` .
- Con WebSockets, solo puede realizar un seguimiento hasta que la solicitud de actualización se realice correctamente.

Registro de llamadas a la API del Equilibrador de carga de aplicación mediante AWS CloudTrail

Elastic Load Balancing está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Elastic Load Balancing. CloudTrail captura todas las llamadas a la API de Elastic Load Balancing como eventos. Las llamadas capturadas incluyen llamadas desde AWS Management Console y llamadas de código

a las operaciones de la API de Elastic Load Balancing. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Elastic Load Balancing. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Elastic Load Balancing, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Para monitorizar otras acciones del equilibrador de carga, como, por ejemplo, cuándo un cliente realiza una solicitud al equilibrador de carga, utilice los registros de acceso. Para obtener más información, consulte Registros de acceso del Equilibrador de carga de aplicación.

Información sobre Elastic Load Balancing en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en Elastic Load Balancing, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su AWS cuenta. Para obtener más información, consulta Cómo ver eventos con el historial de CloudTrail eventos.

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

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

Todas las acciones de Elastic Load Balancing para los balanceadores de carga de aplicaciones se registran CloudTrail y se documentan en la versión 2015-12-01 de referencia de la API. Por ejemplo,

las llamadas a las `DeleteLoadBalancer` acciones `CreateLoadBalancer` y generan entradas en los CloudTrail archivos de registro.

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

- Si la solicitud se realizó con las credenciales raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte el elemento CloudTrailUserIdentity.

Descripción de las entradas del archivo de registros de Elastic Load Balancing

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera, y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un seguimiento ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

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

A continuación, se muestran ejemplos de CloudTrail registros de Elastic Load Balancing para un usuario que creó un Application Load Balancer y, a continuación, lo eliminó mediante. AWS CLI Puede identificar la CLI mediante los elementos `userAgent`. Puede identificar las llamadas al API solicitadas mediante los `eventName`. Encontrará la información sobre el usuario (`Alice`) en el elemento `userIdentity`.

Example Ejemplo: CreateLoadBalancer


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "application",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
```

```
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Example Ejemplo: DeleteLoadBalancer

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

Solución de problemas de Equilibrador de carga de aplicación

La siguiente información puede ayudarle a solucionar problemas del Equilibrador de carga de aplicación.

Problemas

- Un destino registrado no está operativo
- 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"
- El equilibrador de carga muestra tiempos de procesamiento elevados
- El equilibrador de carga envía un código de respuesta 000
- El equilibrador de carga genera un error HTTP
- Hay un destino que genera un error HTTP
- No hay ningún AWS Certificate Manager certificado disponible para su uso
- No se admiten encabezados de varias líneas
- Solucione los problemas de los objetivos en mal estado mediante el mapa de recursos

Un destino registrado no está operativo

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

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

Hay un grupo de seguridad que no permite el tráfico

> El grupo de seguridad asociado a una instancia debe permitir el tráfico del equilibrador de carga a través del puerto de comprobación de estado y el protocolo de comprobación de estado. Puede

agregar una regla a la instancia del grupo de seguridad que permita todo el tráfico procedente del grupo de seguridad del equilibrador de carga. Además, el grupo de seguridad del equilibrador de carga debe permitir el tráfico dirigido a las instancias.

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

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

La ruta de ping no existe

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

Se ha agotado el tiempo de espera de conexión

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

El destino no devuelve un código de respuesta correcto

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

El código de respuesta del destino tenía un formato incorrecto o se produjo un error al conectarse al destino

Comprueba que tu aplicación responde a las solicitudes de comprobación de estado del equilibrador de carga. Algunas aplicaciones requieren una configuración adicional para responder a las comprobaciones de estado, como una configuración de host virtual para responder al encabezado de host HTTP enviado por el equilibrador de carga. El valor del encabezado del host contiene la dirección IP privada del objetivo, seguida del puerto de comprobación de estado

cuando no se utiliza un puerto predeterminado. Si el destino usa un puerto de verificación de estado predeterminado, el valor del encabezado del host contiene solo la dirección IP privada del destino. Por ejemplo, si la dirección IP privada de tu objetivo es `10.0.0.10` y su puerto de comprobación de estado es`8080`, el encabezado HTTP del host enviado por el balanceador de cargas en las comprobaciones de estado sí lo es`Host: 10.0.0.10:8080`. Si la dirección IP privada de tu objetivo es `10.0.0.10` y su puerto de comprobación de estado es, `80` entonces el encabezado HTTP del host enviado por el balanceador de cargas en las comprobaciones de estado sí lo es. `Host: 10.0.0.10` Es posible que se necesite una configuración de host virtual para responder a ese host, o una configuración predeterminada, para comprobar correctamente el estado de la aplicación. Las solicitudes de comprobación de estado tienen los siguientes atributos: `User-Agent` se establece en `ELB-HealthChecker/2.0`, el terminador de línea de los campos del encabezado del mensaje es la secuencia CRLF y el encabezado termina en la primera línea vacía seguida de un CRLF.

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

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

El equilibrador de carga expuesto a Internet está conectado a una subred privada

Debe especificar las subredes públicas para el equilibrador de carga. Una subred pública tiene una ruta hacia la puerta de enlace de Internet de la nube privada virtual (VPC).

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

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

El equilibrador de carga no recibe las solicitudes enviadas a un dominio personalizado

Si el equilibrador de carga no recibe las solicitudes enviadas a un dominio personalizado, compruebe lo siguiente:

El nombre de dominio personalizado no se resuelve en la dirección IP del equilibrador de carga

- Confirme en qué dirección IP se resuelve el nombre de dominio personalizado mediante una interfaz de línea de comandos.
  - Linux, macOS o Unix: puede utilizar el comando `dig` dentro de Terminal. Ej.`dig example.com`
  - Windows: puede utilizar el comando `nslookup` dentro del símbolo del sistema. Ej.`nslookup example.com`
- Confirme en qué dirección IP se resuelve el nombre de DNS del equilibrador de carga mediante una interfaz de línea de comandos.
- Compare ambos resultados. Las direcciones IP deben coincidir.

Si utiliza Route 53 para alojar su dominio personalizado, consulte Mi dominio no está disponible en Internet en la Guía para desarrolladores de Amazon Route 53.

Las solicitudes HTTPS que se envían al equilibrador de carga devuelven “NET: :ERR_CERT_COMMON_NAME_INVALID”

Si las solicitudes HTTPS reciben `NET::ERR_CERT_COMMON_NAME_INVALID` del equilibrador de carga, compruebe las siguientes causas posibles:

- El nombre de dominio utilizado en la solicitud HTTPS no coincide con el nombre alternativo especificado en el certificado ACM asociado a los oyentes.
- Se utiliza el nombre de DNS predeterminado del equilibrador de carga. El nombre de DNS predeterminado no se puede utilizar para realizar solicitudes HTTPS, ya que no se puede solicitar un certificado público para el dominio `*.amazonaws.com`.

El equilibrador de carga muestra tiempos de procesamiento elevados

El equilibrador de carga cuenta los tiempos de procesamiento de forma diferente según la configuración.

- Si AWS WAF está asociado a tu Application Load Balancer y un cliente envía una solicitud HTTP POST, el tiempo de envío de los datos de las solicitudes POST se refleja en el

`request_processing_time` campo de los registros de acceso al balanceador de carga. Este comportamiento se espera para solicitudes HTTP POST.

- Si no AWS WAF está asociado a tu Application Load Balancer y un cliente envía una solicitud HTTP POST, el tiempo de envío de los datos de las solicitudes POST se refleja en el `target_processing_time` campo de los registros de acceso al balanceador de carga. Este comportamiento se espera para solicitudes HTTP POST.

El equilibrador de carga envía un código de respuesta 000

Con las conexiones HTTP/2, si la longitud comprimida de cualquiera de los encabezados supera los 8 KB o si la cantidad de solicitudes enviadas mediante una conexión superan las 10,000, el equilibrador de carga envía un marco GOAWAY y cierra la conexión con un TCP FIN.

El equilibrador de carga genera un error HTTP

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

Errores

- HTTP 400: Solicitud errónea
- HTTP 401: No autorizado
- HTTP 403: Prohibido
- HTTP 405: Método no permitido
- HTTP 408: Request timeout
- HTTP 413: Carga demasiado grande
- HTTP 414: URI demasiado largo
- HTTP 460
- HTTP 463
- HTTP 464
- HTTP 500: Error interno del servidor
- HTTP 501: No implementado
- HTTP 502: Bad puerta de enlace
- HTTP 503: Service unavailable

- HTTP 504: Gateway timeout
- HTTP 505: Versión no compatible
- HTTP 507: almacenamiento insuficiente
- HTTP 561: No autorizado

HTTP 400: Solicitud errónea

Causas posibles:

- El cliente envió una solicitud incorrecta que no se ajusta a la especificación de HTTP.
- El encabezado de la solicitud supera los 16 KB por línea de solicitud, los 16 KB por línea de encabezado o los 64 KB en el conjunto del encabezado.
- El cliente cerró la conexión antes de enviar el cuerpo completo de la solicitud.

HTTP 401: No autorizado

Ha configurado una regla del oyente para autenticar a los usuarios, pero se cumple alguna de las condiciones siguientes:

- Configuró `OnUnauthenticatedRequest` para denegar el acceso a los usuarios no autenticados o el IdP denegó el acceso.
- El tamaño de las notificaciones devueltas por el IdP supera el tamaño máximo admitido por el equilibrador de carga.
- Un cliente ha enviado una solicitud HTTP/1.0 sin encabezado de host y el equilibrador de carga no pudo generar una URL de redirección.
- El ámbito de la solicitud no devuelve un token de ID.
- No se finaliza el proceso de inicio de sesión antes de que caduque el tiempo de espera para iniciar sesión del cliente. Para obtener más información, consulte Tiempo de espera para iniciar sesión en el cliente.

HTTP 403: Prohibido

Configuró una lista de control de acceso AWS WAF web (ACL web) para monitorear las solicitudes a su Application Load Balancer y esta bloqueó una solicitud.

HTTP 405: Método no permitido

El cliente utilizó el método TRACE, que no es compatible con el Equilibrador de carga de aplicación.

HTTP 408: Request timeout

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

HTTP 413: Carga demasiado grande

Causas posibles:

- El destino es una función de Lambda y el cuerpo de la solicitud supera 1 MB.
- El encabezado de la solicitud supera los 16 KB por línea de solicitud, los 16 KB por línea de encabezado o los 64 KB en el conjunto del encabezado.

HTTP 414: URI demasiado largo

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

HTTP 460

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

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

HTTP 463

El equilibrador de carga recibió un encabezado de solicitud X-Forwarded-For con demasiadas direcciones IP. El límite máximo de direcciones IP es de 30.

HTTP 464

El equilibrador de carga recibió un protocolo de solicitudes entrantes que no es compatible con la configuración de versiones del protocolo del grupo de destino.

Causas posibles:

- El protocolo de solicitud es HTTP/1.1, mientras que la versión del protocolo del grupo de destino es gRPC o HTTP/2.
- El protocolo de solicitud es un gRPC, mientras que la versión del protocolo del grupo de destino es un HTTP/1.1.
- El protocolo de solicitud es HTTP/2 y la solicitud no es POST, mientras que la versión del protocolo del grupo de destino es un gRPC.

HTTP 500: Error interno del servidor

Causas posibles:

- Configuró una lista de control de acceso AWS WAF web (ACL web) y se produjo un error al ejecutar las reglas de la ACL web.
- El equilibrador de carga no puede comunicarse con el punto de conexión del token de IdP o el punto de conexión de información de usuario de IdP.
  - Compruebe que el DNS del IdP se pueda resolver públicamente.
  - Verifique que los grupos de seguridad de su equilibrador de carga y las ACL de red de su VPC permiten el acceso saliente a estos puntos de enlace.
  - Compruebe que la VPC tiene acceso a Internet. Si hay un equilibrador de carga interno, utilice una puerta de enlace NAT para permitirle que obtenga acceso a Internet.
- La reclamación del usuario recibida del IdP tiene un tamaño superior a 11 KB.

HTTP 501: No implementado

El equilibrador de carga recibió un encabezado Transfer-Encoding con un valor no admitido. Los valores admitidos para Transfer-Encoding son `chunked` e `identity`. Como alternativa, puede utilizar el encabezado Content-Encoding.

HTTP 502: Bad puerta de enlace

Causas posibles:

- El equilibrador de carga recibió un TCP RST desde el destino cuando intentó establecer una conexión.
- El equilibrador de carga recibió una respuesta inesperada del destino, como, por ejemplo, "ICMP Destination unreachable (Host unreachable) (Destino de ICMP inaccesible (Host de destino inaccesible))", al intentar establecer una conexión. Compruebe si se permite el tráfico desde las subredes del equilibrador de carga a los destinos del puerto de destino.
- El destino cerró las conexiones con un TCP RST o un TCP FIN mientras que el equilibrador de carga tenía una solicitud pendiente en el destino. Compruebe si la duración de keep-alive del destino es inferior al valor del tiempo de inactividad del equilibrador de carga.
- La respuesta del destino es incorrecta o contiene encabezados HTTP que no son válidos.
- El encabezado de respuesta destino superó los 32 K para todo el encabezado de respuesta.
- El período de retardo de anulación del registro para una solicitud que se maneja mediante un destino cuyo registro se ha anulado. Aumente el periodo de retraso de manera que las operaciones largas puedan completarse.
- El destino es una función de Lambda y el cuerpo de la respuesta supera 1 MB.
- El destino es una función de Lambda que no respondió antes de que se agotara el tiempo de espera configurado.
- El destino es una función de Lambda que ha devuelto un error o el servicio de Lambda ha limitado la función.
- El balanceador de cargas detectó un error de protocolo de enlace SSL al conectarse a un destino.

Para obtener más información, consulte Cómo solucionar los errores HTTP 502 del Application Load Balancer en el AWS Support Knowledge Center.

HTTP 503: Service unavailable

Los grupos de destino del equilibrador de carga no tienen destinos registrados.

HTTP 504: Gateway timeout

Causas posibles:

- El equilibrador de carga ha establecido una conexión con el destino antes de que se agotara el tiempo de espera de conexión (10 segundos).
- El equilibrador de carga estableció una conexión con el destino, pero el destino no respondió antes de que transcurriera el período de inactividad.
- La ACL de red de la subred no permite el tráfico desde los destinos hasta los nodos del equilibrador de carga en los puertos efímeros (1024-65535).
- El destino devuelve un encabezado de longitud de contenido que es mayor que el cuerpo de la entidad. El equilibrador de carga agotó el tiempo de espera con los bytes restantes.
- El destino es una función de Lambda y el servicio Lambda no respondió antes de que expirara el tiempo de espera de conexión.
- El balanceador de cargas detectó un tiempo de espera del protocolo de enlace SSL (10 segundos) al conectarse a un destino.

HTTP 505: Versión no compatible

El equilibrador de carga recibió una solicitud de versión HTTP inesperada. Por ejemplo, el equilibrador de carga estableció una conexión HTTP/1 pero recibió una solicitud HTTP/2.

HTTP 507: almacenamiento insuficiente

La URL de redireccionamiento es demasiado larga.

HTTP 561: No autorizado

Configuró una regla de oyente para autenticar a los usuarios, pero el IdP devolvió un código de error al autenticar al usuario. Compruebe en sus registros de acceso el código de motivo de error correspondiente.

Hay un destino que genera un error HTTP

El equilibrador de carga reenvía respuestas HTTP válidas desde los destinos al cliente, incluidos los errores HTTP. Los errores HTTP generados por un destino se registran en las métricas `HTTPCode_Target_4XX_Count` y `HTTPCode_Target_5XX_Count`.

No hay ningún AWS Certificate Manager certificado disponible para su uso

Si decide utilizar un agente de escucha HTTPS con su Application Load Balancer AWS Certificate Manager , debe validar la propiedad del dominio antes de emitir un certificado. Si se omite este paso durante la configuración, el certificado permanece en el estado `Pending Validation` y no estará disponible para su uso hasta que se valide.

- Si utiliza la validación por correo electrónico, consulte Validación por correo electrónico en la Guía del usuario de AWS Certificate Manager .
- Si utiliza la validación por correo electrónico, consulte Validación DNS en la Guía del usuario de AWS Certificate Manager .

No se admiten encabezados de varias líneas

Los equilibradores de carga de aplicaciones no admiten encabezados multilínea, incluido el encabezado de tipo de medio `message/http`. Cuando se proporciona un encabezado multilínea, el Equilibrador de carga de aplicación añade un carácter de dos puntos, "`:`", antes de pasarlo al destino.

Solucione los problemas de los objetivos en mal estado mediante el mapa de recursos

Si los objetivos de Application Load Balancer no superan las comprobaciones de estado, puede utilizar el mapa de recursos para encontrar los objetivos en mal estado y tomar medidas en función del código del motivo del error. Para obtener más información, consulte Mapa de recursos de Application Load Balancer.

El mapa de recursos ofrece dos vistas: vista general y mapa objetivo en mal estado. La vista general está seleccionada de forma predeterminada y muestra todos los recursos del balanceador de cargas. Al seleccionar la vista del mapa de objetivos en mal estado, solo se mostrarán los objetivos en mal estado de cada grupo de objetivos asociado al Application Load Balancer.

> **Note**
>
> Debe activar Mostrar detalles de los recursos para ver el resumen de la comprobación de estado y los mensajes de error de todos los recursos aplicables del mapa de recursos. Si no está activado, debe seleccionar cada recurso para ver sus detalles.

La columna Grupos objetivo muestra un resumen de los objetivos saludables y no saludables de cada grupo objetivo. Esto puede ayudar a determinar si todos los objetivos no están pasando los controles de estado o si solo algunos objetivos específicos están fallando. Si todos los objetivos de un grupo objetivo no superan las comprobaciones de estado, compruebe la configuración del grupo objetivo. Seleccione el nombre de un grupo objetivo para abrir su página de detalles en una pestaña nueva.

La columna TargetID muestra el TargetID y el estado actual de la comprobación de estado de cada objetivo. Cuando un objetivo no está en buen estado, se muestra el código del motivo del error en la comprobación de estado. Cuando un solo objetivo no supere una comprobación de estado, compruebe que el objetivo tenga recursos suficientes y confirme que las aplicaciones que se ejecutan en el destino estén disponibles. Seleccione el ID de un objetivo para abrir su página de detalles en una pestaña nueva.

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

Comprueba que tu instancia no supere las comprobaciones de estado y, a continuación, comprueba el código del motivo de la falla para detectar los siguientes problemas:

- Insalubre: la respuesta HTTP no coincide
  - Compruebe que la aplicación que se ejecuta en el destino envíe la respuesta HTTP correcta a las solicitudes de comprobación de estado del balanceador de carga de aplicaciones.
  - Como alternativa, puedes actualizar la solicitud de comprobación de estado del balanceador de carga de aplicaciones para que coincida con la respuesta de la aplicación que se ejecuta en el destino.
- Incorrecto: se agotó el tiempo de espera de la solicitud
  - Compruebe que los grupos de seguridad y las listas de control de acceso a la red (ACL) asociados a sus objetivos y a Application Load Balancer no bloqueen la conectividad.

- Compruebe que el destino tenga suficientes recursos disponibles para aceptar conexiones desde Application Load Balancer.
- Compruebe el estado de todas las aplicaciones que se estén ejecutando en el destino.
- Las respuestas a las comprobaciones de estado del balanceador de carga de aplicaciones se pueden ver en los registros de aplicaciones de cada objetivo. Para obtener más información, consulta los códigos de motivo de Health Check.

- Insalubre: FailedHealthChecks
  - Compruebe el estado de todas las aplicaciones que se estén ejecutando en el destino.
  - Compruebe que el objetivo esté escuchando el tráfico en el puerto de comprobación de estado.

    Cuando se utiliza un agente de escucha HTTPS

    Usted elige qué política de seguridad se utilizará para las conexiones front-end. La política de seguridad utilizada para las conexiones de back-end se selecciona automáticamente en función de la política de seguridad de front-end que se utilice.

    - Si su agente de escucha HTTPS utiliza una política de seguridad TLS 1.3 para las conexiones front-end, la política de seguridad se utiliza para las conexiones `ELBSecurityPolicy-TLS13-1-0-2021-06` back-end.
    - Si su agente de escucha HTTPS no utiliza una política de seguridad de TLS 1.3 para las conexiones front-end, la política de seguridad se utiliza para las conexiones back-end. `ELBSecurityPolicy-2016-08`

    Para obtener más información, consulte Políticas de seguridad.
  - Compruebe que el destino proporciona un certificado y una clave de servidor en el formato correcto especificado en la política de seguridad.
  - Compruebe que el destino admita uno o más cifrados coincidentes y un protocolo proporcionado por Application Load Balancer para establecer protocolos de enlace TLS.

Cuotas de los equilibradores de carga de aplicaciones

La cuenta de AWS tiene cuotas predeterminadas para cada servicio de AWS (estas cuotas anteriormente se denominaban “límites”). A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de los equilibradores de carga de aplicaciones, abra la consola de Service Quotas. En el panel de navegación, seleccione Servicios de AWS y elija Elastic Load Balancing. También puedes usar el comando describe-account-limits(AWS CLI) para Elastic Load Balancing.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no está disponible en Service Quotas, utilice el formulario de aumento del límite de Elastic Load Balancing.

Equilibradores de carga

La cuenta de AWS incluye las siguientes cuotas en relación con los equilibradores de carga de aplicaciones.

Nombre	Valor predeterminado	Ajustable
Equilibradores de carga de aplicaciones por región	50	Sí
Certificados por Equilibrador de carga de aplicación (sin incluir los certificados predeterminados)	25	Sí
Oyentes por Equilibrador de carga de aplicación	50	Sí
Grupos destino por acción por Equilibrador de carga de aplicación	5	No
Grupos de destino por equilibrador de carga de aplicaciones	100	No
Destinos por Equilibrador de carga de aplicación	1 000	Sí

Grupos de destino

Las cuotas siguientes son para grupos de destino.

Nombre	Valor predeterminado	Ajustable
Grupos de destino por región	3000*	Sí
Destinos por grupo de destino por región (instancias o direcciones IP)	1 000	Sí
Destinos por grupo de destino por región (funciones de Lambda)	1	No
Equilibradores de carga por grupo de destino	1	No

* Esta cuota se comparte entre los equilibradores de carga de aplicaciones y los Equilibradores de carga de red.

Reglas

Las siguientes cuotas son para reglas.

Nombre	Valor predeterminado	Ajustable
Reglas por Equilibrador de carga de aplicación (no se incluyen las reglas predeterminadas)	100	Sí
Valores de condición por regla	5	No
Caracteres comodín de condición por regla	5	No
Evaluaciones de coincidencia por regla	5	No

Confía en las tiendas

Las siguientes cuotas son para tiendas de confianza.

Nombre	Valor predeterminado	Ajustable
Confíe en las tiendas por cuenta	20	Sí
Número de oyentes que utilizan mTLS en modo de verificación, por balanceador de carga.	2	No

Certificados de la autoridad de certificación

Las cuotas siguientes son para los certificados de CA.

Nombre	Valor predeterminado	Ajustable
Certificados de CA por almacén de confianza	25	Sí
Tamaño del certificado de CA	16 KB	No
Profundidad máxima de la cadena de certificados	4	No

Listas de revocación de certificados

Las cuotas siguientes son para las listas de revocación de certificados.

Nombre	Valor predeterminado	Ajustable
Listas de revocación por almacén de confianza	30	Sí
Entradas de revocación por almacén de confianza	500.000	Sí
Tamaño del archivo de la lista de revocaciones	50 MB	No

Encabezados HTTP

A continuación se presentan los límites de tamaño para los encabezados HTTP.

Nombre	Valor predeterminado	Ajustable
Línea de solicitud	16 K	No
Encabezado único	16 K	No
Encabezado de respuesta completo	32 K	No
Encabezado de solicitud completo	64 K	No

Historial de revisión de los equilibrador de carga de aplicaciones

En la tabla siguiente, se describen las versiones de los equilibradores de carga de aplicaciones.

Cambio	Descripción	Fecha
Mapa de recursos	En esta versión, se añade la posibilidad de ver los recursos y las relaciones del balanceador de cargas en un formato visual.	8 de marzo de 2024
WAF con un clic	Esta versión añade soporte para configurar el comportamiento del balanceador de carga si se integra con un solo clic. AWS WAF	6 de febrero de 2024
TLS mutuo	Esta versión añade compatibilidad con la autenticación TLS mutua.	26 de noviembre de 2023
Pesos objetivo automáticos	Esta versión añade compatibilidad con el algoritmo automático de ponderaciones objetivo.	26 de noviembre de 2023
Terminación FIPS 140-3 TLS	Esta versión añade políticas de seguridad que utilizan módulos criptográficos FIPS 140-3 al finalizar las conexiones TLS.	20 de noviembre de 2023
Registre los destinos mediante IPv6	Esta versión añade compatibilidad con el registro de instancias como destinos	2 de octubre de 2023

	cuando se direcciona mediante IPv6.	
Políticas de seguridad compatibles con TLS 1.3	Esta versión añade compatibilidad con las políticas de seguridad predefinidas de TLS 1.3.	22 de marzo de 2023
Cambio de zona	Esta versión añade soporte para desviar el tráfico de una única zona de disponibilidad dañada mediante la Amazon Route 53 Application Recovery Controller integración con.	28 de noviembre de 2022
Desactive el equilibrio de carga entre zonas	Esta versión añade compatibilidad para desactivar el equilibrio de carga entre zonas.	28 de noviembre de 2022
Estado del grupo de destino	Esta versión permite configurar el recuento o el porcentaje mínimo de destinos que deben estar en buen estado y las acciones que debe realizar el equilibrador de carga cuando no se alcanza el umbral.	28 de noviembre de 2022
Equilibrio de carga entre zonas	Esta versión añade soporte para configurar el equilibrio de carga entre zonas a nivel del grupo objetivo.	17 de noviembre de 2022
Grupos de destino IPv6	Esta versión añade compatibilidad con la configuración de grupos de destino de IPv6 para los equilibradores de carga de aplicaciones.	23 de noviembre de 2021

Equilibradores de carga internos de IPv6	Esta versión añade compatibilidad con la configuración de grupos de destino de IPv6 para los equilibradores de carga de aplicaciones.	23 de noviembre de 2021
AWS PrivateLink y direcciones IP estáticas	Esta versión admite el uso AWS PrivateLink y la exposición de direcciones IP estáticas al reenviar el tráfico directamente desde los balanceadores de carga de red a los balanceadores de carga de aplicaciones.	27 de septiembre de 2021
Preservación del puerto del cliente	Esta versión agrega un atributo para preservar el puerto de origen que el cliente utiliza para conectarse al equilibrador de carga.	29 de julio de 2021
Encabezados TLS	Esta versión agrega un atributo para indicar que los encabezados de TLS, que contienen información sobre la versión de TLS negociada y el conjunto de cifrado, se agregan a la solicitud del cliente antes de enviarla al destino.	21 de julio de 2021
Certificados de ACM adicionales	Esta versión es compatible con los certificados RSA con longitudes de clave de 2048, 3072 y 4096 bits, y con todos los certificados ECDSA.	14 de julio de 2021

Persistencia en función de la aplicación	En esta versión, se añade una cookie en función de aplicaciones para admitir sesiones persistentes en el equilibrador de carga.	8 de febrero de 2021
Política de seguridad para FS compatible con la versión 1.2 de TLS	Esta versión incorpora una política de seguridad para Forward Secrecy (FS) compatible con la versión 1.2 de TLS.	24 de noviembre de 2020
No se puede abrir el soporte para WAF	Esta versión añade soporte para configurar el comportamiento del balanceador de cargas si se integra con él. AWS WAF	13 de noviembre de 2020
Compatibilidad con gRPC y HTTP/2	Esta versión añade compatibilidad con cargas de trabajo de gRPC y HTTP/2. end-to-end	29 de octubre de 2020
Soporte para Outpost	Puede aprovisionar un Application Load Balancer en su. AWS Outposts	8 de septiembre de 2020
Modo de mitigación de desincronización	En esta versión se agrega compatibilidad con el modo de mitigación de desincronización.	17 de agosto de 2020
Solicitudes menos pendientes	Esta versión añade soporte para el algoritmo de solicitudes menos pendientes.	25 de noviembre de 2019

Grupos de destino ponderados	Esta versión incorpora compatibilidad con acciones de reenvío con varios grupos de destino. Las solicitudes se distribuyen a estos grupos de destino en función de la ponderación especificada para cada grupo de destino.	19 de noviembre de 2019
New attribute (Nuevo atributo)	Esta versión incorpora compatibilidad con el atributo routing.http.drop_invalid_header_fields.enabled.	15 de noviembre de 2019
Políticas de seguridad para FS	Esta versión añade compatibilidad con tres políticas de seguridad adicionales predefinidas de confidencialidad directa.	8 de octubre de 2019
Direccionamiento de solicitudes avanzado	Esta versión añade compatibilidad para tipos de condición adicionales para las reglas de oyente.	27 de marzo de 2019
Funciones de Lambda como destino	Esta versión añade compatibilidad para registrar funciones de Lambda como destino.	29 de noviembre de 2018
Acciones de redirección	Esta versión incorpora la compatibilidad con el equilibrador de carga para redirigir las solicitudes a una URL diferente.	25 de julio de 2018

Acciones de respuesta fija	Esta versión incorpora la compatibilidad con el equilibrador de carga para devolver una respuesta HTTP personalizada.	25 de julio de 2018
Políticas de seguridad para FS y TLS 1.2	Esta versión añade soporte para dos políticas de seguridad predefinidas adicionales.	6 de junio de 2018
Autenticación del usuario	Esta versión añade soporte para que el equilibrador de carga pueda autenticar a los usuarios de sus aplicaciones utilizando sus identidades corporativas o sociales antes de las solicitudes de direccionamiento.	30 de mayo de 2018
Permisos de nivel de recursos	Esta versión añade soporte para permisos en el nivel de recursos y claves de condición de etiquetado.	10 de mayo de 2018
Modo de inicio lento	Esta versión añade soporte para el modo de inicio lento, que aumenta gradualmente la cuota de solicitudes que el equilibrador de carga envía a un destino recién registrado mientras se calienta.	24 de marzo de 2018
Compatibilidad con SNI	Esta versión incorpora soporte para Indicación de nombre de servidor (SNI).	10 de octubre de 2017

Direcciones IP como destinos	Esta versión añade soporte para registrar direcciones IP como destinos.	31 de agosto de 2017
Enrutamiento basado en host	Esta versión añade soporte para las solicitudes de direccionamiento basadas en los nombres de host del encabezado de host.	5 de abril de 2017
Políticas de seguridad para TLS 1.1 y TLS 1.2	En esta versión, se han añadido las políticas de seguridad de TLS 1.1 y TLS 1.2.	6 de febrero de 2017
Compatibilidad con IPv6	En esta versión se agrega compatibilidad con las direcciones IPv6.	25 de enero de 2017
Rastreo de solicitudes	En esta versión se agrega compatibilidad con el rastreo de solicitudes.	22 de noviembre de 2016
Soporte de percentiles para la métrica TargetResponseTime	Esta versión añade compatibilidad con las nuevas estadísticas de percentiles admitidas por Amazon. CloudWatch	17 de noviembre de 2016
Tipo de equilibrador de carga nuevo	Esta versión de Elastic Load Balancing presenta los equilibradores de carga de aplicaciones.	11 de agosto de 2016

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.