aws

Network Load Balancers

Elastic Load Balancing

Elastic Load Balancing: Network Load Balancers

Table of Contents

¿Qué es un equilibrador de carga de red?

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 red. Para obtener más información sobre los demás equilibradores de carga, consulte la Guía del usuario sobre equilibradores de carga de aplicación, 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 red

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

Un agente de escucha comprueba las solicitudes de conexión de los clientes, utilizando el protocolo y el puerto configurados, y reenvía las solicitudes a un grupo de destino.

Un grupo de destino direcciona las solicitudes a uno o varios destinos registrados, como instancias de EC2, mediante el protocolo y el número de puerto que ha especificado. Los grupos de destino del equilibrador de carga de red admiten los protocolos TCP, UDP, TCP_UDP, TLS, QUIC y TCP_QUIC. 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 realizan en todos los destinos registrados en los grupos de destino que se especifican en la acción predeterminada del equilibrador de carga.

Para obtener más información, consulte la documentación siguiente:

- Equilibradores de carga

- Oyentes
- Grupos de destino

Información general sobre el equilibrador de carga de red

Un equilibrador de carga de red actúa como la cuarta capa del modelo de interconexión de sistemas abiertos (OSI). Puede gestionar millones de solicitudes por segundo. Después de que el equilibrador de carga recibe una solicitud de un cliente, selecciona un destino de un grupo de destino en la acción predeterminada. Intenta enviar la solicitud al destino seleccionado mediante el protocolo y el puerto especificados.

Cuando se habilita una zona de disponibilidad para el equilibrador de carga, Elastic Load Balancing crea en ella un nodo de equilibrador de carga en la zona de disponibilidad. De manera predetermina, cada nodo del balanceador de carga distribuye el tráfico entre los destinos registrados en su zona de disponibilidad solamente. Si habilita el balanceo de carga entre zonas, cada nodo del balanceador de carga distribuye el tráfico equitativamente entre los destinos registrados en todas las zonas de disponibilidad habilitadas. Para obtener más información, consulte Actualización de las zonas de disponibilidad del equilibrador de carga de red.

A fin de aumentar la tolerancia a fallas de sus aplicaciones, puede habilitar varias zonas de disponibilidad para el equilibrador de carga y asegurarse de que cada grupo de destino tenga al menos un destino en cada zona de disponibilidad habilitada. Por ejemplo, si uno o varios grupos de destino no tienen un destino en buen estado en una zona de disponibilidad, se quita del DNS la dirección IP de la subred correspondiente, pero los nodos del balanceador de carga de las demás zonas de disponibilidad siguen estando disponibles para dirigir el tráfico. Si un cliente no respeta el tiempo de vida (TTL) y envía solicitudes a la dirección IP una vez que se ha eliminado de DNS, las solicitudes producen errores.

Para el tráfico TCP, el balanceador de carga selecciona un destino utilizando un algoritmo hash de flujo, en función del protocolo, la dirección IP de origen, el puerto de origen, la dirección IP de destino, el puerto de destino y el número de secuencia TCP. Las conexiones TCP desde un cliente tienen distintos puertos de origen y números de secuencia y se pueden dirigir a diferentes destinos. Cada conexión TCP individual se dirige a un único destino durante la conexión.

Para el tráfico UDP, el balanceador de carga selecciona un destino utilizando un algoritmo hash de flujo, en función del protocolo, la dirección IP de origen, el puerto de origen, la dirección IP de destino y el puerto de destino. Un flujo UDP tiene el mismo origen y destino, por lo que se redirige siempre

a un único destino durante su vida útil. Los flujos UDP distintos tienen puertos y direcciones IP de origen diferentes, por lo que se pueden dirigir a destinos distintos.

Para el tráfico QUIC, el equilibrador de carga selecciona un destino mediante el ID de servidor especificado en el ID de conexión (CID). Para los intentos iniciales de conexión que no incluyen un ID de servidor, se utiliza un algoritmo hash de flujo basado en el protocolo, la dirección IP de origen, el puerto de origen, la dirección IP de destino y el puerto de destino. Una vez que se establece un ID de conexión, el tráfico de este CID se enruta al mismo destino durante toda la vigencia del CID.

Elastic Load Balancing crea una interfaz de red para cada zona de disponibilidad que habilita. Cada nodo de balanceador de carga de la zona de disponibilidad utiliza esta interfaz de red para obtener una dirección IP estática. Al crear un balanceador de carga expuesto a Internet, puede asociar una dirección IP elástica por cada subred.

Al crear un grupo de destino, debe especificar su tipo de destino, que determina cómo se registran los destinos. Por ejemplo, puede registrar los ID de instancia, las direcciones IP o un equilibrador de carga de aplicación. El tipo de destino también afecta a si se preservan las direcciones IP del cliente. Para obtener más información, consulte the section called “Preservación de la IP del cliente”.

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.

Beneficios de migrar desde un equilibrador de carga clásico

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

- Capacidad para gestionar cargas de trabajo volátiles y escalar hasta millones de solicitudes por segundo.
- Compatibilidad con direcciones IP estáticas para el balanceador de carga. También puede asignar una dirección IP elástica por subred habilitada para el balanceador de carga.

- Compatibilidad con el registro de destinos por dirección IP, incluidos los destinos situados fuera de la VPC para el equilibrador de carga.
- Compatibilidad con el direccionamiento de solicitudes a varias aplicaciones en una sola instancia EC2. Puede registrar cada instancia o dirección IP con el mismo grupo de destino utilizando varios puertos.
- Compatibilidad con las aplicaciones en contenedores. Amazon Elastic Container Service (Amazon ECS) permite seleccionar un puerto no utilizado al programar una tarea y registrarla en un grupo de destino mediante este puerto. De este modo, puede hacer un uso eficiente de los clústeres.
- Compatibilidad con el monitoreo independiente del estado de cada servicio, pues las comprobaciones de estado se definen para cada grupo de destino y muchas métricas de Amazon CloudWatch se notifican también para cada grupo de destino. Si adjunta un grupo de destino a un grupo de escalado automático, podrá escalar cada servicio de forma dinámica en función de la demanda.
- Compatibilidad con los protocolos QUIC y TCP_QUIC, con control avanzado de la congestión, establecimiento de conexión con menos viajes de ida y vuelta, TLS integrado y migración de conexiones entre redes.

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

Introducción

Para crear un equilibrador de carga de red mediante Consola de administración de AWS, AWS CLI o AWS CloudFormation, consulte Crear un Equilibrador de carga de red.

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

Precios

Para obtener más información, consulte Precios de Elastic Load Balancing.

Network Load Balancers

Un equilibrador de carga de red actúa como único punto de contacto para los clientes. Los clientes envían las solicitudes al equilibrador de carga de red y este se las envía a los destinos, tales como instancias de EC2, de una o varias zonas de disponibilidad.

Para configurar el equilibrador de carga de red, debe crear grupos de destino y, a continuación, registrar los destinos en los grupos de destino. El equilibrador de carga de red es más eficaz si se asegura de que cada zona de disponibilidad habilitada tenga al menos un destino registrado. También puede crear agentes de escucha para comprobar la existencia de solicitudes de conexión de los clientes y direccionar las solicitudes de los clientes a los destinos de sus grupos de destino.

Los equilibradores de carga de red admiten las conexiones de clientes a través de una interconexión con VPC, VPN administradas por AWS, Direct Connect y soluciones de VPN de terceros.

Contenido

- Reservas de capacidad para el equilibrador de carga de red

Estado del equilibrador de carga

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

`provisioning`

El equilibrador de carga de red se está configurando.

`active`

El equilibrador de carga de red se ha configurado completamente y está listo para enrutar tráfico.

`failed`

El equilibrador de carga de red no se ha podido configurar.

Tipo de dirección IP

Puede establecer los tipos de direcciones IP que los clientes pueden utilizar con el equilibrador de carga de red.

Los equilibradores de carga de red admiten los siguientes tipos de direcciones IP:

`ipv4`

Los clientes se deben conectar mediante direcciones IPv4 (por ejemplo, 192.0.2.1).

`dualstack`

Los clientes pueden conectarse al equilibrador de carga de red 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 de red se comunica con los destinos en función del tipo de dirección IP del grupo de destino.
- Para admitir la conservación de la dirección IP de origen para oyentes UDP IPv6, asegúrese de que Habilitar prefijo para NAT de origen IPv6 esté activado.

- Cuando se habilita el modo de doble pila para el equilibrador de carga de red, Elastic Load Balancing proporciona un registro de DNS AAAA para el equilibrador de carga de red. Los clientes que se comunican con el equilibrador de carga de red mediante direcciones IPv4 resuelven el registro de DNS A. Los clientes que se comunican con el equilibrador de carga de red mediante direcciones IPv6 resuelven el registro de DNS AAAA.
- El acceso al equilibrador de carga de red de doble pila interno a través de la puerta de enlace de Internet está bloqueado para evitar el acceso no deseado a Internet. Sin embargo, esto no impide otros accesos a Internet (por ejemplo, mediante interconexión, Transit Gateway, AWS Direct Connect o Site-to-Site VPN).

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

Tiempo de inactividad de conexión

Para cada solicitud de TCP que un cliente realiza a través de un equilibrador de carga de red, se controla el estado de la conexión. Si transcurre el tiempo de inactividad sin que ni el cliente ni el destino envíen datos a través de la conexión, se deja de realizar un seguimiento de esta. Si un cliente o destino envía datos una vez transcurrido el tiempo de inactividad, el cliente recibe un paquete RST TCP para indicar que la conexión ya no es válida.

El valor de tiempo de inactividad predeterminado para los flujos TCP es de 350 segundos, pero se puede actualizar a cualquier valor comprendido entre 60 y 6000 segundos. Los clientes o destinos pueden utilizar paquetes keepalive TCP para reiniciar el tiempo de inactividad. Los paquetes keepalive que se han enviado para mantener las conexiones de TLS no pueden contener datos ni carga útil.

El tiempo de espera de inactividad de la conexión para los oyentes TLS es de 350 segundos y no se puede modificar. Cuando un oyente de TLS recibe un paquete keepalive de TCP de un cliente o un destino, el equilibrador de carga genera paquetes keepalive de TCP y los envía a las conexiones de frontend y backend cada 20 segundos. No puede modificar este comportamiento.

Si bien UDP no tiene conexión, el equilibrador de carga mantiene el estado del flujo de UDP en función de los puertos y las direcciones IP de origen y destino. Esto garantiza que los paquetes que pertenecen al mismo flujo se envíen de forma consistente al mismo destino. Una vez transcurrido el tiempo de inactividad, el equilibrador de carga considera el paquete de UDP entrante como un flujo nuevo y lo dirige a un destino nuevo. Elastic Load Balancing establece el valor del tiempo de inactividad para los flujos de UDP en 120 segundos. Esto no se puede cambiar.

Las instancias EC2 deben responder a una nueva solicitud en un plazo de 30 segundos para establecer una ruta de retorno.

Para obtener más información, consulte Actualización del tiempo de inactividad.

Atributos del equilibrador de carga

Puede configurar el equilibrador de carga de red editando sus atributos. Para obtener más información, consulte Edición de atributos del equilibrador de carga.

A continuación se muestran los atributos de equilibrador de carga para equilibradores de carga de red:

`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 Requisitos del bucket.

`access_logs.s3.prefix`

Prefijo de la ubicación en el bucket de Amazon S3.

`deletion_protection.enabled`

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

`ipv6.deny_all_igw_traffic`

Bloquea el acceso de una puerta de enlace de Internet (IGW) al equilibrador de carga de red, lo que evita accesos no intencionados al equilibrador de carga de red interno a través de una puerta de enlace de Internet. Se configura como `false` para los equilibradores de carga de red con acceso a Internet y como `true` para los equilibradores de carga de red internos. Este atributo no impide el acceso a Internet que no sea de IGW (por ejemplo, mediante interconexión, Transit Gateway, AWS Direct Connect o Site-to-Site VPN).

`load_balancing.cross_zone.enabled`

Indica si el balance de carga entre zonas está habilitado. El valor predeterminado es `false`.

`dns_record.client_routing_policy`

Indica cómo se distribuye el tráfico entre las zonas de disponibilidad de los equilibradores de carga de red. Los valores posibles son `availability_zone_affinity` con una afinidad de zona del 100 por ciento, `partial_availability_zone_affinity` con una afinidad de zona del 85 por ciento y `any_availability_zone` con una afinidad de zona del 0 por ciento.

`secondary_ips.auto_assigned.per_subnet`

El número de direcciones IP secundarias que se deben configurar. Use este valor para resolver errores de asignación de puertos si no puede agregar destinos. El intervalo válido es de 0 a 7. El valor predeterminado es 0. Una vez que establezca este valor, no se puede reducir.

`zonal_shift.config.enabled`

Indica si el cambio de zona está habilitado. El valor predeterminado es `false`.

Balance de carga entre zonas

De manera predetermina, cada nodo del equilibrador de carga de red distribuye el tráfico entre los destinos registrados en su zona de disponibilidad únicamente. Si activa el equilibrio de carga entre zonas, cada nodo del equilibrador de carga de red distribuye el tráfico entre los destinos registrados en todas las zonas de disponibilidad habilitadas. También puede activar el equilibrio de carga entre zonas a nivel del grupo de destino. Para obtener más información, consulte the section called "Balance de carga entre zonas" y Equilibrio de carga entre zonas en la Guía del usuario de Elastic Load Balancing.

Nombre de DNS

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

Si prefiere utilizar un nombre de DNS que sea más fácil de recordar, puede crear un nombre de dominio personalizado y asociarlo al nombre de DNS del equilibrador de carga de red. Cuando un cliente realiza una solicitud utilizando este nombre de dominio personalizado, el servidor DNS lo convierte en el nombre de DNS del equilibrador de carga de red.

En primer lugar, registre un nombre de dominio con un registrador de nombres de dominio acreditado. A continuación, utilice su servicio de DNS (por ejemplo, su registrador de dominio) para

crear un registro de DNS y enrutar las solicitudes al equilibrador de carga de red. Para obtener más información, consulte la documentación de su servicio de DNS. Por ejemplo, si utiliza Amazon Route 53 como servicio de DNS, se crea un registro de alias que apunta al equilibrador de carga de red. Para obtener más información, consulte Enrutamiento del tráfico a un equilibrador de carga de ELB en la Guía para desarrolladores de Amazon Route 53.

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

Linux o Mac

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

Windows

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

El equilibrador de carga de red tiene registros de DNS para sus nodos. Puede utilizar nombres de DNS con la siguiente sintaxis para determinar las direcciones IP de los nodos del equilibrador de carga de red: *az*.*name*-*id*.elb.*region*.amazonaws.com.

Linux o Mac

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

Windows

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

Estado zonal del equilibrador de carga

Los equilibradores de carga de red tienen registros de DNS y direcciones IP zonales en Route 53 para cada zona de disponibilidad habilitada. Cuando un equilibrador de carga de red no supera una comprobación de estado zonal para una zona de disponibilidad concreta, su registro de DNS se elimina de Route 53. El estado zonal del equilibrador de carga se monitorea mediante la métrica

`ZonalHealthStatus` de Amazon CloudWatch, lo que brinda más información sobre los eventos que provocan una conmutación por error para implementar medidas preventivas y garantizar una disponibilidad óptima de las aplicaciones. Para obtener más información, consulte Métricas del balanceador de carga de red.

Los equilibradores de carga de red pueden no superar las comprobaciones de estado zonales por múltiples motivos, lo que provoca que pasen a encontrarse en mal estado. Consulte a continuación las causas más comunes que provocan el mal estado de los equilibradores de carga de red debido a la no superación de las comprobaciones de estado zonales.

Compruebe las siguientes causas posibles:

- No hay destinos en buen estado para el equilibrador de carga
- El número de destinos en buen estado es inferior al mínimo configurado
- Existe un cambio de zona o un cambio automático de zona en curso
- Se está desplazado automáticamente el tráfico a zonas en buen estado debido a problemas detectados

Crear un Equilibrador de carga de red

Un equilibrador de carga de red toma las solicitudes de los clientes y las distribuye entre los destinos de un grupo de destino; por ejemplo, instancias de EC2. Para obtener más información, consulte la the section called “Información general sobre el equilibrador de carga de red”.

Tareas

- Requisitos previos
- Creación del equilibrador de carga
- Cómo probar el equilibrador de carga
- Pasos a seguir a continuación

Requisitos previos

- Decida qué zonas de disponibilidad y tipos de direcciones IP admitirá la aplicación. Configure la VPC del equilibrador de carga con subredes en cada una de estas zonas de disponibilidad. Si la aplicación admite tráfico IPv4 e IPv6, asegúrese de que las subredes tengan CIDR tanto IPv4 como IPv6. Implemente al menos un destino en cada zona de disponibilidad.

- Asegúrese de que los grupos de seguridad de las instancias de destino permitan el tráfico en el puerto del oyente desde las direcciones IP de los clientes (si los destinos se especifican mediante el ID de instancia) o desde los nodos del equilibrador de carga (si los destinos se especifican por dirección IP). Para obtener más información, consulte the section called “Grupos de seguridad de destino”.
- Asegúrese de que los grupos de seguridad de las instancias de destino permitan el tráfico desde el equilibrador de carga en el puerto de comprobación de estado con el protocolo de comprobación de estado.
- Si planea proporcionar direcciones IP estáticas al equilibrador de carga, asegúrese de que cada dirección IP elástica proceda del grupo de direcciones IPv4 de Amazon y pertenezca al mismo grupo de fronteras de red que el equilibrador de carga.
- Si planea utilizar oyentes QUIC o TCP_QUIC, asegúrese de que el equilibrador de carga de red use el tipo de dirección `ipv4` y que no tenga grupos de seguridad asociados.

Creación del equilibrador de carga

Como parte de la creación de un equilibrador de carga de red, creará el equilibrador de carga, al menos un oyente y al menos un grupo de destino. El equilibrador de carga está listo para gestionar solicitudes de los clientes cuando existe al menos un destino registrado y en buen estado en cada una de sus zonas de disponibilidad habilitadas.

Console

Para crear un equilibrador de carga de red

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 Crear un equilibrador de carga.
4. En Equilibrador de carga de red, elija Crear.
5. Configuración básica

   a. En Nombre del balanceador de carga, escriba un nombre para el equilibrador de carga de red. El nombre debe ser único dentro del conjunto de equilibradores de carga en la región. Puede tener un máximo de 32 caracteres y solo puede contener caracteres alfanuméricos y guiones. No puede comenzar ni terminar con un guion ni con `internal-`.

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

c. En Tipo de dirección IP del equilibrador de carga, seleccione IPv4 si los clientes usan direcciones IPv4 para comunicarse con el equilibrador de carga de red, o Doble pila si los clientes usan tanto direcciones IPv4 como IPv6 para comunicarse con el equilibrador de carga de red.

6. Asignación de redes

a. En VPC, seleccione la VPC que preparó para el equilibrador de carga. Cuando se utiliza un equilibrador de carga de acceso a Internet, solo se pueden seleccionar VPC que tengan una puerta de enlace de Internet.

b. Con un equilibrador de carga de doble pila, no puede agregar un oyente UDP a menos que Habilitar prefijo para NAT de origen IPv6 esté Activado (prefijos de NAT de origen por subred).

c. En Zonas de disponibilidad y subredes, seleccione al menos una zona de disponibilidad y seleccione una subred por zona. Las subredes que se han compartido con usted están disponibles para su selección.

   Al seleccionar varias zonas de disponibilidad y registrar destinos en cada una de ellas, se mejora la tolerancia a errores de la aplicación.

d. Con un equilibrador de carga orientado a Internet, puede seleccionar una dirección IP elástica para cada zona de disponibilidad. Esto proporciona al balanceador de carga direcciones IP estáticas.

   Con un equilibrador de carga interno, puede introducir una dirección IPv4 privada dentro del rango de direcciones de cada subred o permitir que AWS seleccione una en su nombre.

   Con un equilibrador de carga de pila doble, puede introducir una dirección IPv6 dentro del rango de direcciones de cada subred o permitir que AWS seleccione una en su nombre.

   En el caso de un equilibrador de carga con NAT de origen habilitado, puede introducir un prefijo IPv6 personalizado o permitir que AWS seleccione uno en su nombre.

7. Grupos de seguridad

Preseleccionamos el grupo de seguridad predeterminado para la VPC del equilibrador de carga. Puede seleccionar grupos de seguridad adicionales según sea necesario. Si no tiene un grupo de seguridad que cumpla con sus requisitos, elija crear un nuevo grupo de seguridad para crearlo ahora. Para obtener más información, consulte Crear un grupo de seguridad en la Guía del usuario de Amazon VPC.

> **Warning**
>
> Si no asocia ahora ningún grupo de seguridad al equilibrador de carga de red, no podrá asociarlo más adelante.

> **Warning**
>
> Para utilizar oyentes QUIC o TCP_QUIC, el equilibrador de carga de red no debe tener grupos de seguridad.

8. Los oyentes y el enrutamiento

   a. De forma predeterminada, el oyente acepta tráfico de TCP en el puerto 80. Puede conservar la configuración predeterminada del oyente o modificar el Protocolo o y el Puerto según sea necesario.

   b. En Acción predeterminada, seleccione un grupo de destino al que reenviar el tráfico.

      Para agregar otro grupo de destino, elija Agregar grupo de destino y actualice las ponderaciones según sea necesario.

      Si no tiene un grupo de destino que se ajuste a sus necesidades, seleccione Crear grupo de destino para crear uno ahora. Para obtener más información, consulte Creación de un grupo de destino..

   c. (Opcional) Elija Agregar etiqueta del oyente e introduzca una clave de etiqueta y un valor de etiqueta.

   d. (Opcional) Elija Agregar oyente para agregar otro oyente (por ejemplo, un oyente TLS).

9. Configuración de oyente seguro

   Esta sección aparece solo si agrega un oyente TLS.

a. En Política de seguridad, elija una política de seguridad que cumpla con sus requisitos. Para obtener más información, consulte Políticas de seguridad.

b. En Certificado de servidor SSL/TLS predeterminado, seleccione Desde ACM como origen del certificado. Seleccione un certificado que haya aprovisionado o importado mediante AWS Certificate Manager. Si no tiene un certificado disponible en ACM, pero sí dispone de un certificado para usar con su equilibrador de carga, seleccione Importar certificado y proporcione la información requerida. De lo contrario, elija Solicitar un certificado de ACM. Para obtener más información, consulte Certificados AWS Certificate Manager en la Guía del usuario de AWS Certificate Manager.

c. (Opcional) En Política ALPN, seleccione una política para habilitar ALPN. Para obtener más información, consulte the section called “Políticas de ALPN”.

10. Etiquetas del equilibrador de carga

    (Opcional) Amplíe Etiquetas del equilibrador de carga. Elija Agregar nueva etiqueta e introduzca una clave de etiqueta y un valor de etiqueta. Para obtener más información, consulte Etiquetas.

11. Resumen

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

AWS CLI

Para crear un equilibrador de carga de red

Utilice el comando create-load-balancer.

En el siguiente ejemplo, se crea un equilibrador de carga de acceso a Internet con dos zonas de disponibilidad habilitadas y un grupo de seguridad.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para crear un equilibrador de carga de red interno

Incluya la opción `--scheme` como se muestra en el siguiente ejemplo.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para crear un equilibrador de carga de red de pila doble

Incluya la opción `--ip-address-type` como se muestra en el siguiente ejemplo.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --ip-address-type dualstack \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para agregar un agente de escucha

Utilice el comando create-listener. Para ver ejemplos, consulte Creación de un oyente.

CloudFormation

Para crear un equilibrador de carga de red

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
```

```
        - !Ref mySecurityGroup
      Tags:
        - Key: 'department'
          Value: '123'
```

Para agregar un agente de escucha

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::Listener. Para ver ejemplos, consulte Creación de un oyente.

Cómo probar el equilibrador de carga

Después de crear el equilibrador de carga de red, puede verificar que las instancias de EC2 hayan superado la comprobación de estado inicial y, a continuación, comprobar que el equilibrador de carga les envía tráfico. Para eliminar el equilibrador de carga de red, consulte Eliminar un equilibrador de carga de red.

Para probar el equilibrador de carga de red

1. Una vez creado el equilibrador de carga de red, seleccione Cerrar.
2. En el panel de navegación izquierdo, elija Grupos de destino.
3. Seleccione el nuevo grupo de destino.
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 en buen estado. Cuando al menos una instancia esté en buen estado, podrá probar el equilibrador de carga de red. Para obtener más información, consulte Estado del destino.
5. En el panel de navegación, seleccione Equilibradores de carga.
6. Seleccione el nuevo equilibrador de carga de red.
7. Copie el nombre de DNS del equilibrador de carga de red (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.

Pasos a seguir a continuación

Después de crear el equilibrador de carga, es posible que desee realizar las siguientes acciones:

- Configurar los atributos del equilibrador de carga.
- Configurar los atributos del grupo de destino.
- [Oyentes TLS] Agregue certificados a la lista de certificados opcionales.
- Configurar las características de supervisión.

Actualización de las zonas de disponibilidad del equilibrador de carga de red

Puede habilitar o desactivar las zonas de disponibilidad del equilibrador de carga de red en cualquier momento. Cuando habilita una zona de disponibilidad, debe especificar una subred de esa zona de disponibilidad. 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. La habilitación de varias zonas de disponibilidad ayuda a mejorar la tolerancia a errores de las aplicaciones.

Elastic Load Balancing crea un nodo del equilibrador de carga de red en la zona de disponibilidad que seleccione y una interfaz de red para la subred seleccionada en esa zona de disponibilidad. Cada nodo del equilibrador de carga de red en la zona de disponibilidad utiliza la interfaz de red para obtener una dirección IPv4. Puede ver estas interfaces de red, pero no se pueden modificar.

Consideraciones

- En el caso de los equilibradores de carga de red con acceso a Internet, las subredes que especifique deben tener al menos 8 direcciones IP disponibles. En el caso de los equilibradores de carga de red internos, este requisito solo es necesario si permite que AWS seleccione una dirección IPv4 privada de la subred.
- No puede especificar una subred en una zona de disponibilidad restringida. No obstante, puede especificar una subred en una zona de disponibilidad no restringida y utilizar el equilibrio de carga entre zonas para distribuir el tráfico hacia los destinos en la zona de disponibilidad restringida.
- No se puede especificar una subred en una zona local.
- No puede eliminar una subred si el equilibrador de carga de red tiene asociaciones activas con puntos de conexión de VPC de Amazon.
- Al volver a agregar una subred eliminada anteriormente, se crea una nueva interfaz de red con un ID diferente.

- Los cambios de subred dentro de la misma zona de disponibilidad se deben realizar como acciones independientes. Primero debe completar la eliminación de la subred existente y, a continuación, puede agregar la nueva subred.
- La eliminación de una subred puede tardar hasta 3 minutos en completarse.

Al crear un equilibrador de carga de red orientado a Internet, puede optar por especificar una dirección IP elástica para cada zona de disponibilidad. Las direcciones IP elásticas proporcionan direcciones IP estáticas al equilibrador de carga de red. Si decide no especificar una dirección IP elástica, AWS asignará una dirección IP elástica para cada zona de disponibilidad.

Al crear un equilibrador de carga de red interno, puede optar por especificar una dirección IP privada de cada subred. Las direcciones IP privadas proporcionan direcciones IP estáticas al equilibrador de carga de red. Si decide no especificar una dirección IP privada, AWS asigna una en su nombre.

Antes de actualizar las zonas de disponibilidad del equilibrador de carga de red, recomendamos que evalúe cualquier posible impacto en las conexiones existentes, los flujos de tráfico o las cargas de trabajo de producción.

⚠ La actualización de una zona de disponibilidad puede resultar disruptiva

- Cuando se elimina una subred, se elimina su interfaz de red elástica (ENI) asociada. Esto provoca que se terminen todas las conexiones activas en la zona de disponibilidad.
- Después de eliminar una subred, todos los destinos dentro de la zona de disponibilidad con la que estaba asociada se marcan como `unused`. Como resultado, esos destinos se eliminan del grupo de destinos disponibles y se terminan todas las conexiones activas hacia estos destinos. Esto incluye cualquier conexión que se origine en otras zonas de disponibilidad cuando se utiliza el equilibrio de carga entre zonas.
- Los equilibradores de carga de red tienen un tiempo de vida (TTL) de 60 segundos para su nombre de dominio completo (FQDN). Cuando se elimina una zona de disponibilidad que contiene destinos activos, las conexiones de cliente existentes pueden experimentar tiempos de espera hasta que se vuelva a producir la resolución DNS, y el tráfico se redirige a las zonas de disponibilidad restantes.

Console

Para modificar las zonas de disponibilidad

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. Seleccione Save changes (Guardar cambios).

AWS CLI

Para modificar las zonas de disponibilidad

Utilice el comando set-subnets.

```
aws elbv2 set-subnets \
    --load-balancer-arn load-balancer-arn \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890
```

CloudFormation

Para modificar las zonas de disponibilidad

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
```

```
        - !Ref new-subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Actualización de los tipos de direcciones IP para el equilibrador de carga de red

Puede configurar el equilibrador de carga de red para que los clientes puedan comunicarse con él solo mediante direcciones IPv4 o bien mediante direcciones IPv4 e IPv6 (pila doble). El equilibrador de carga de red 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 cuando cree el equilibrador de carga de red y actualizarlo en cualquier momento.
- La nube privada virtual (VPC) y las subredes que especifique para el equilibrador de carga de red 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 de las subredes del equilibrador de carga de red deben enrutar tráfico IPv6.
- Las ACL de red de las subredes del equilibrador de carga de red deben permitir el tráfico IPv6.
- No hay oyentes QUIC ni TCP_QUIC asociados al equilibrador de carga de red.

Console

Para actualizar el tipo de dirección IP

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 la casilla de verificación del equilibrador de carga de red.
4. Elija Actions, Edit IP address type.
5. En Tipo de dirección IP, elija IPv4 para admitir únicamente las direcciones IPv4, o bien Doble pila para admitir las direcciones IPv4 e IPv6.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar el tipo de dirección IP

Utilice el comando set-ip-address-type.

```
aws elbv2 set-ip-address-type \
    --load-balancer-arn load-balancer-arn \
    --ip-address-type dualstack
```

CloudFormation

Para actualizar el tipo de dirección IP

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Edición de atributos del equilibrador de carga de red

Después de crear el equilibrador de carga de red, puede editar sus atributos.

Atributos del equilibrador de carga

- Protección contra eliminación
- Balance de carga entre zonas
- Afinidad de DNS de la zona de disponibilidad
- Direcciones IP secundarias

Protección contra eliminación

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

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

Console

Para habilitar o desactivar la protección contra eliminación

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 de red para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Bajo Protección, habilite o desactive Protección contra eliminación.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar o desactivar la protección contra eliminación

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

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=deletion_protection.enabled,Value=true"
```

CloudFormation

Para habilitar o desactivar la protección contra eliminación

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer para incluir el atributo `deletion_protection.enabled`.

```
Resources:
  myLoadBalancer:
```

```
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "deletion_protection.enabled"
          Value: "true"
```

Balance de carga entre zonas

Con los equilibradores de carga de red, el equilibrio de carga entre zonas está desactivado de forma predeterminada en el nivel del equilibrador de carga, pero puede activarlo en cualquier momento. 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. Para obtener más información, consulte the section called “Balance de carga entre zonas”.

Console

Para habilitar o desactivar el equilibrio de carga entre zonas para un equilibrador de carga

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 el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar los atributos del equilibrador de carga, active o desactive el Equilibrio de carga entre zonas.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar o desactivar el equilibrio de carga entre zonas para un equilibrador de carga

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

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Para habilitar o desactivar el equilibrio de carga entre zonas para un equilibrador de carga

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer para incluir el atributo `load_balancing.cross_zone.enabled`.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Afinidad de DNS de la zona de disponibilidad

Si utiliza la política de enrutamiento de clientes predeterminada, las solicitudes que se envíen al nombre de DNS del equilibrador de carga de red recibirán cualquier dirección IP del equilibrador de carga de red que esté en buen estado. Esto hace que se distribuyan las conexiones de los clientes entre las zonas de disponibilidad del equilibrador de carga de red. Con las políticas de enrutamiento por afinidad de zona de disponibilidad, las consultas de DNS de los clientes prefieren las direcciones IP de los equilibradores de carga de red de su propia zona de disponibilidad. Esto ayuda a mejorar tanto la latencia como la resiliencia, ya que los clientes no necesitan cruzar los límites de la zona de disponibilidad para conectarse a los destinos.

Las políticas de enrutamiento por afinidad de zona de disponibilidad solo se aplican a los clientes que resuelven el nombre de DNS del equilibrador de carga de red mediante Route 53 Resolver. Para obtener más información, consulte ¿Qué es Amazon Route 53 Resolver? en la Guía para desarrolladores de Amazon Route 53.

Políticas de enrutamiento de clientes disponibles para los equilibradores de carga de red que utilizan Route 53 Resolver:

- Afinidad de zona de disponibilidad: afinidad de zona del 100 por ciento

  Las consultas de DNS de los clientes darán preferencia a la dirección IP del equilibrador de carga de red de su propia zona de disponibilidad. Las consultas se pueden resolver en otras zonas si no existen direcciones IP del equilibrador de carga de red en buen estado de su propia zona.
- Afinidad de zona de disponibilidad parcial: afinidad de zona del 85 por ciento

  El 85 % de las consultas de DNS de los clientes darán preferencia a las direcciones IP del equilibrador de carga de red de su propia zona de disponibilidad, mientras que el resto de las consultas se resuelven en cualquier zona en buen estado. Las consultas se pueden resolver en otras zonas en buen estado si no hay direcciones IP en buen estado en su zona. Si no hay direcciones IP en buen estado en ninguna zona, las consultas se resuelven en cualquier zona.
- Cualquier zona de disponibilidad (predeterminada): afinidad de zona del 0 por ciento

  Las consultas de DNS de los clientes se resuelven entre las direcciones IP del equilibrador de carga de red en buen estado en todas las zonas de disponibilidad del equilibrador de carga de red.

La afinidad de zona de disponibilidad ayuda a enrutar las solicitudes del cliente al equilibrador de carga de red, mientras que el equilibrio de carga entre zonas se utiliza para ayudar a enrutar las solicitudes desde el equilibrador de carga hacia los destinos. Cuando se utiliza la afinidad de zona de disponibilidad, se debe desactivar el equilibrio de carga entre zonas; esto garantiza que el tráfico del equilibrador de carga de red desde los clientes hacia los destinos permanezca dentro de la misma zona de disponibilidad. Con esta configuración, el tráfico de los clientes se envía a la zona de disponibilidad del mismo equilibrador de carga de red, por lo que se recomienda configurar la aplicación para que escale de manera independiente en cada zona de disponibilidad. Esta consideración es importante cuando el número de clientes por cada zona de disponibilidad o el tráfico por cada zona de disponibilidad no son iguales. Para obtener más información, consulte Equilibrio de carga entre zonas para grupos de destino.

Cuando se considera que una zona de disponibilidad se encuentra en mal estado o cuando se inicia un cambio de zona, la dirección IP de zona se considerará en mal estado y no se devolverá a los clientes a menos que se produzca un error de apertura. La afinidad de zona de disponibilidad se mantiene cuando se produce un error al abrir el registro de DNS. Esto ayuda a mantener la independencia de las zonas de disponibilidad y a evitar posibles errores entre las zonas.

Cuando se utiliza la afinidad de zona de disponibilidad, se esperan tiempos de desequilibrio entre las zonas de disponibilidad. Se recomienda asegurarse de que los destinos se escalen a nivel de zona para admitir la carga de trabajo de cada zona de disponibilidad. En los casos en que estos desequilibrios sean significativos, se recomienda desactivar la afinidad de zona de disponibilidad. Esto permite una distribución uniforme de las conexiones de los clientes entre todas las zonas de disponibilidad del equilibrador de carga de red en 60 segundos, o el TTL de DNS.

Antes de utilizar la afinidad de zona de disponibilidad, tenga en cuenta lo siguiente:

- La afinidad de zona de disponibilidad provoca cambios en todos los clientes de los equilibradores de carga de red que utilizan Route 53 Resolver.
  - Los clientes no pueden decidir entre las resoluciones de DNS locales de la zona y de varias zonas. La afinidad de zona de disponibilidad decide por ellos.
  - Los clientes no disponen de un método fiable para determinar cuándo se ven afectados por la afinidad de zona de disponibilidad ni cómo saber qué dirección IP se encuentra en cada zona de disponibilidad.
- Al utilizar la afinidad de zona de disponibilidad con los equilibradores de carga de red y Route 53 Resolver, recomendamos que los clientes utilicen el punto de conexión entrante de Route 53 Resolver en su propia zona de disponibilidad.
- Los clientes permanecerán asignados a su dirección IP local de la zona hasta que se considere que se encuentra en mal estado en función de las comprobaciones de estado del DNS y se elimine del DNS.
- El uso de la afinidad de zona de disponibilidad con el equilibrio de carga entre zonas activado puede provocar una distribución desequilibrada de las conexiones de los clientes entre las zonas de disponibilidad. Se recomienda configurar la pila de aplicaciones para que se escale de forma independiente en cada zona de disponibilidad, a fin de garantizar que pueda admitir el tráfico de clientes de zona.
- Si el equilibrio de carga entre zonas se encuentra activado, el equilibrador de carga de red está sujeto a un impacto entre zonas.

- La carga en cada una de las zonas de disponibilidad de los equilibradores de carga de red será proporcional a las ubicaciones de zona de las solicitudes de los clientes. Si no configura cuántos clientes se ejecutan en cada zona de disponibilidad, tendrá que escalar de forma independiente cada zona de disponibilidad de forma reactiva.

Monitorización

Se recomienda realizar un seguimiento de la distribución de las conexiones entre las zonas de disponibilidad mediante las métricas del equilibrador de carga de red de la zona. Puede utilizar las métricas para ver la cantidad de conexiones nuevas y activas por zona.

Recomendamos que realice un seguimiento de lo siguiente:

- **`ActiveFlowCount`** – la cantidad total de flujos (o conexiones) simultáneos de clientes a destinos.
- **`NewFlowCount`** – la cantidad total de flujos (o conexiones) nuevos establecidos desde los clientes a los destinos en el periodo indicado.
- **`HealthyHostCount`** – la cantidad de destinos que se considera que se encuentran en buen estado.
- **`UnHealthyHostCount`** – la cantidad de destinos que se considera que no se encuentran en buen estado.

Para obtener más información, consulte Métricas de CloudWatch para el equilibrador de carga de red

Habilitación de la afinidad de zona de disponibilidad

Console

Para habilitar la afinidad de zona de disponibilidad

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 de red para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración del enrutamiento de zonas de disponibilidad, Política de enrutamiento de clientes (registro de DNS), seleccione Afinidad de zona de disponibilidad o Afinidad de zona de disponibilidad parcial.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar la afinidad de zona de disponibilidad

Use el comando modify-load-balancer-attributes con el atributo `dns_record.client_routing_policy`.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes
 "Key=dns_record.client_routing_policy,Value=partial_availability_zone_affinity"
```

CloudFormation

Para habilitar la afinidad de zona de disponibilidad

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer para incluir el atributo `dns_record.client_routing_policy`.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "dns_record.client_routing_policy"
          Value: "partial_availability_zone_affinity"
```

Direcciones IP secundarias

Si experimenta errores de asignación de puertos y no puede agregar destinos al grupo de destino para resolverlos, puede agregar direcciones IP secundarias a las interfaces de red del equilibrador de carga. Para cada zona en la que el equilibrador de carga esté habilitado, seleccionamos

direcciones IPv4 de la subred del equilibrador de carga y las asignamos a la interfaz de red correspondiente. Estas direcciones IP secundarias se utilizan para establecer conexiones con los destinos. También se utilizan para el tráfico de comprobaciones de estado. Recomendamos agregar una dirección IP secundaria inicialmente, supervisar la métrica `PortAllocationErrors` y agregar otra dirección IP secundaria solo si los errores de asignación de puertos no se resuelven.

> **Warning**
>
> Después de agregar direcciones IP secundarias, no es posible eliminarlas. La única forma de liberar las direcciones IP secundarias es eliminar el equilibrador de carga. Antes de agregar direcciones IP secundarias, verifique que haya suficientes direcciones IPv4 disponibles en las subredes del equilibrador de carga.

Console

Para agregar una dirección IP secundaria

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 de red para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Expanda Atributos de casos especiales, desbloquee el atributo Direcciones IP secundarias asignadas automáticamente por subred y seleccione la cantidad de direcciones IP secundarias.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para agregar una dirección IP secundaria

Use el comando modify-load-balancer-attributes con el atributo `secondary_ips.auto_assigned.per_subnet`.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=secondary_ips.auto_assigned.per_subnet,Value=1"
```

Puede utilizar el comando describe-network-interfaces para obtener las direcciones IPv4 de las interfaces de red del equilibrador de carga. El parámetro `--filters` limita los resultados a las interfaces de red de los equilibradores de carga de red, y el parámetro `--query` restringe aún más los resultados al equilibrador de carga con el nombre especificado y muestra únicamente los campos indicados. Puede incluir cualquier campos adicionales según sea necesario.

```
aws elbv2 describe-network-interfaces \
    --filters "Name=interface-type,Values=network_load_balancer" \
    --query "NetworkInterfaces[?contains(Description,'my-nlb')].
{ID:NetworkInterfaceId,AZ:AvailabilityZone,Addresses:PrivateIpAddresses[*]}"
```

CloudFormation

Para agregar una dirección IP secundaria

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer para incluir el atributo `secondary_ips.auto_assigned.per_subnet`.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "secondary_ips.auto_assigned.per_subnet"
          Value: "1"
```

Actualización de los grupos de seguridad del equilibrador de carga de red

Puede asociar un grupo de seguridad al equilibrador de carga de red para controlar el tráfico que tiene permitido llegar y salir del equilibrador de carga de red. Debe especificar los puertos, los

protocolos y los orígenes para permitir el tráfico entrante y los puertos, protocolos y destinos a fin de permitir el tráfico saliente. Si no asigna un grupo de seguridad al equilibrador de carga de red, todo el tráfico de los clientes puede llegar a los oyentes del equilibrador de carga de red y todo el tráfico puede salir de este.

Puede agregar una regla a los grupos de seguridad asociados a sus destinos que haga referencia al grupo de seguridad asociado a su equilibrador de carga de red. Esto permite que los clientes envíen tráfico a los destinos a través del equilibrador de carga de red, pero impide que envíen tráfico a los destinos directamente. Hacer referencia al grupo de seguridad asociado al equilibrador de carga de red en los grupos de seguridad asociados a los destinos garantiza que estos últimos acepten el tráfico del equilibrador de carga de red incluso si habilita la preservación de la IP del cliente para el equilibrador de carga de red.

No se le cobrará por el tráfico que se encuentre bloqueado por las reglas del grupo de seguridad entrante.

Contenido

Consideraciones

- Puede asociar grupos de seguridad a un equilibrador de carga de red al crearlo. Si crea un equilibrador de carga de red sin asociarle ningún grupo de seguridad, no podrá asociárselos al equilibrador de carga de red más adelante. Se recomienda asociar un grupo de seguridad al equilibrador de carga de red cuando se cree este.
- Después de crear un equilibrador de carga de red con grupos de seguridad asociados, puede cambiar los grupos de seguridad asociados al equilibrador de carga de red en cualquier momento.
- Las comprobaciones de estado se encuentran sujetas a las reglas de salida, pero no a las de entrada. Debe asegurarse de que las reglas de salida no bloqueen el tráfico de la comprobación de estado. De lo contrario, el equilibrador de carga de red considera que los destinos se encuentran en mal estado.

- Puede controlar si el tráfico de PrivateLink se encuentra sujeto a las reglas de entrada. Si habilita las reglas de entrada en el tráfico de PrivateLink, el origen del tráfico es la dirección IP privada del cliente, no la interfaz del punto de conexión.

Ejemplo: Filtrar el tráfico de clientes

Las siguientes reglas de entrada del grupo de seguridad asociado a su equilibrador de carga de red solo permiten el tráfico que proviene del rango de direcciones especificado. Si se trata de un equilibrador de carga de red interno, puede especificar un rango de CIDR de VPC como origen para permitir solo el tráfico de una determinada VPC. Si se trata de un equilibrador de carga de red con acceso a Internet que debe aceptar tráfico desde cualquier parte de Internet, puede especificar 0.0.0.0/0 como origen.

Entrada

Protocolo	Origen	Intervalo de puertos	Comment
protocolo	*rango de direcciones IP del cliente*	*puerto del oyente*	Permite el tráfico entrante desde el CIDR de origen en el puerto del oyente
ICMP	0.0.0.0/0	Todos	Permite que el tráfico de ICMP entrante sea compatible con MTU o la Detección de la MTU de la ruta †

† Para obtener más información, consulte Detección de la MTU de la ruta en la Guía del usuario de Amazon EC2.

Salida

Protocolo	Destino	Intervalo de puertos	Comment
Todos	Cualquier lugar	Todos	Permite todo el tráfico de salida

Ejemplo: Aceptar tráfico solo procedente del equilibrador de carga de red

Suponga que su equilibrador de carga de red cuenta con un grupo de seguridad sg-111112222233333. Utilice las siguientes reglas en los grupos de seguridad asociados a sus instancias de destino para asegurarse de que solo acepten tráfico del equilibrador de carga de red. Debe asegurarse de que los destinos acepten tráfico procedente del equilibrador de carga de red tanto en el puerto de destino como en el puerto de comprobación de estado. Para obtener más información, consulte the section called “Grupos de seguridad de destino”.

Entrada

Protocolo	Origen	Intervalo de puertos	Comment
protocolo	sg-111112222233333	*puerto de destino*	Permite tráfico entrante procedente del equilibrador de carga de red en el puerto de destino
protocolo	sg-111112222233333	*comprobación de estado*	Permite tráfico entrante procedente del equilibrador de carga de red en el puerto de comprobación de estado

Salida

Protocolo	Destino	Intervalo de puertos	Comment
Todos	Cualquier lugar	Cualquiera	Permite todo el tráfico de salida

Actualizar los grupos de seguridad asociados

Si asoció al menos un grupo de seguridad a un equilibrador de carga de red cuando lo creó, puede actualizar los grupos de seguridad de ese equilibrador de carga de red en cualquier momento.

Console

Para actualizar los grupos de seguridad

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 equilibrador de carga de red.
4. En la pestaña Seguridad, seleccione Editar.
5. Para asociar un grupo de seguridad al equilibrador de carga de red, selecciónelo. Para eliminar un grupo de seguridad del equilibrador de carga de red, desmárquelo.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar los grupos de seguridad

Utilice el comando set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --security-groups sg-1234567890abcdef0 sg-0abcdef0123456789
```

CloudFormation

Para actualizar los grupos de seguridad

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
        - !Ref myNewSecurityGroup
```

Actualizar la configuración de seguridad

De manera predeterminada, aplicamos las reglas de entrada del grupo de seguridad a todo el tráfico enviado al equilibrador de carga de red. No obstante, es posible que no desee aplicar estas reglas al tráfico enviado al equilibrador de carga de red a través de AWS PrivateLink, ya que puede provenir de direcciones IP superpuestas. En tal caso, puede configurar el equilibrador de carga de red para que no apliquemos las reglas de entrada al tráfico enviado al equilibrador de carga red a través de AWS PrivateLink.

Console

Para actualizar la configuración de seguridad

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 equilibrador de carga de red.
4. En la pestaña Seguridad, seleccione Editar.
5. En Configuración de seguridad, desmarque Aplicar reglas entrantes en el tráfico PrivateLink.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar la configuración de seguridad

Utilice el comando set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --enforce-security-group-inbound-rules-on-private-link-traffic off
```

CloudFormation

Para actualizar la configuración de seguridad

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
```

```
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      EnforceSecurityGroupInboundRulesOnPrivateLinkTraffic: off
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Monitoreo de grupos de seguridad del equilibrador de carga de red

Utilice las métricas de CloudWatch `SecurityGroupBlockedFlowCount_Inbound` y `SecurityGroupBlockedFlowCount_Outbound` para monitorear el número de flujos que bloquean los grupos de seguridad del equilibrador de carga de red. El tráfico bloqueado no se refleja en otras métricas. Para obtener más información, consulte the section called “Métricas de CloudWatch”.

Utilice los registros del flujo de la VPC para monitorear el tráfico que aceptan o rechazan los grupos de seguridad del equilibrador de carga de red. Para obtener más información, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Etiquetado de un equilibrador de carga de red

Las etiquetas ayudan a categorizar los equilibradores de carga de red de diferentes maneras. Por ejemplo, puede etiquetar un recurso por objetivo, propietario o entorno.

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

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

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

Console

Para actualizar las etiquetas de un equilibrador de carga

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 la casilla de verificación del equilibrador de carga de red.
4. En la pestaña Etiquetas, elija Administrar etiquetas.
5. Para agregar una etiqueta, elija Agregar etiqueta e ingrese 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.
6. Para actualizar una etiqueta, introduzca nuevos valores en Clave o Valor.
7. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.
8. Seleccione Save changes (Guardar cambios).

AWS CLI

Para agregar etiquetas de

Utilice el comando add-tags. En el siguiente ejemplo, se agregan dos etiquetas.

```
aws elbv2 add-tags \
    --resource-arns load-balancer-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Para eliminar etiquetas

Utilice el comando remove-tags. En el siguiente ejemplo, se eliminan las etiquetas con las claves especificadas.

```
aws elbv2 remove-tags \
    --resource-arns load-balancer-arn \
    --tag-keys project department
```

CloudFormation

Para agregar etiquetas de

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::LoadBalancer para incluir la propiedad `Tags`.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Eliminar un equilibrador de carga de red

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

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

No se puede eliminar un equilibrador de carga de red si lo está utilizando otro servicio. Por ejemplo, si el equilibrador de carga de red está asociado a un servicio de punto de conexión de VPC, debe eliminar la configuración del servicio de punto de conexión para poder eliminar el equilibrador de carga de red asociado.

Cuando se elimina un equilibrador de carga de red, se eliminan también sus oyentes. Eliminar un equilibrador de carga de red 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 del equilibrador de carga de red.

Console

Para eliminar un equilibrador de carga de red

1. Si cuenta con un registro de DNS para el dominio que señala al equilibrador de carga de red, apúntelo hacia una ubicación nueva y espere a que surta efecto el cambio de DNS antes de eliminar el equilibrador de carga de red. Por 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 Equilibradores de carga.
4. Seleccione la casilla de verificación del equilibrador de carga de red.
5. Seleccione Acciones, Eliminar equilibrador de carga.
6. Cuando se le pida confirmación, ingrese **`confirm`** y elija Eliminar.

AWS CLI

Para eliminar un equilibrador de carga de red

Utilice el comando delete-load-balancer.

```
aws elbv2 delete-load-balancer \
```

```
    --load-balancer-arn load-balancer-arn
```

Visualización del mapa de recursos del equilibrador de carga de red

El mapa de recursos del equilibrador de carga de red proporciona una visualización interactiva de la arquitectura de equilibradores de carga de red, incluyendo sus oyentes, grupos de destino y destinos asociados. Además, el mapa de recursos destaca las relaciones y vías de enrutamiento entre todos los recursos, lo que le ofrece una representación visual de la configuración de equilibradores de carga de red.

Para ver el mapa de recursos del equilibrador de carga

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 de red.
4. Elija la pestaña Resource map (Mapa de recursos).

Componentes del mapa de recursos

Vistas de mapa

Existen dos vistas disponibles en el mapa de recursos del equilibrador de carga de red: Información general y Mapa de destinos en mal estado. Información general está seleccionada de manera predeterminada y muestra todos los recursos del equilibrador de carga de red. Si selecciona la vista Mapa de destinos en mal estado, solo se mostrarán los destinos en mal estado y los recursos asociados a ellos.

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

Columnas de recursos

El mapa de recursos del equilibrador de carga de red contiene tres columnas de recursos, una para cada tipo de recurso. Los grupos de recursos son Agentes de escucha, Grupos de destino y Destinos.

Mosaicos de recursos

Cada recurso dentro de una columna tiene su propio mosaico, que muestra detalles sobre ese recurso concreto.

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

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

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

Exportación del mapa de recursos

Si selecciona Exportar, tiene la opción de exportar la vista actual del mapa de recursos del equilibrador de carga de red en formato PDF.

Registros de CloudWatch para el equilibrador de carga de red

Registros de Amazon CloudWatch admite los registros de acceso del equilibrador de carga de red como registros proporcionados por el servicio, lo que mejora la observabilidad y simplifica la depuración de los patrones de tráfico de red. Puede analizar los registros de acceso del equilibrador de carga de red directamente en CloudWatch para obtener información sobre las conexiones de

cliente, la distribución del tráfico y el estado de las conexiones, lo que ayuda a identificar y resolver problemas de red con mayor rapidez.

Puede configurar la entrega de los registros de acceso del equilibrador de carga de red a Registros de Amazon CloudWatch, Amazon Data Firehose y Amazon Simple Storage Service (Amazon S3), con compatibilidad con el formato Apache Parquet.

> **Important**
>
> Los registros de acceso se crean solo si el equilibrador de carga tiene un oyente TLS y si los registros contienen información acerca de las solicitudes de TLS únicamente. Los registros de acceso registran las solicitudes en la medida de lo posible. Recomendamos utilizar los registros de acceso para comprender la naturaleza de las solicitudes y no como una relación exhaustiva de todas las solicitudes.

> **Important**
>
> Los registros de acceso “heredados” aún están disponibles para el equilibrador de carga de red. Para administrar las configuraciones de los registros de acceso heredados, visite la pestaña Atributos del equilibrador de carga. Para obtener más información sobre los registros de acceso heredados, consulte Registros de acceso para el equilibrador de carga de red.

Con esta integración con Registros de CloudWatch, puede realizar el seguimiento detallado de los patrones de acceso mediante consultas de Información de registros de CloudWatch, crear filtros de métricas para la supervisión y revisar los patrones de tráfico en tiempo real mediante Live Tail.

Puede habilitar Registros de CloudWatch para los registros de acceso del equilibrador de carga de red desde la pestaña Integraciones del equilibrador de carga en la consola. Para habilitar el registro, debe iniciar sesión como un usuario que tenga determinados permisos. Además, debe conceder permisos a AWS para permitir el envío de los registros.

Para conocer los permisos necesarios para cada destino de registro, consulte Habilitación del registro desde los servicios de AWS.

Para obtener más información, consulte ¿Qué es Registros de Amazon CloudWatch? .

Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Cambio de zona del equilibrador de carga de red

El cambio de zona es una prestación del Controlador de recuperación de aplicaciones (ARC) de Amazon. Con el cambio de zona, puede mover un recurso del equilibrador de carga de red 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.

Cuando inicia un cambio de zona, el equilibrador de carga de red deja de enrutar tráfico hacia los destinos en la zona de disponibilidad afectada. Las conexiones existentes con destinos en la zona de disponibilidad afectada no se terminan como resultado del cambio de zona. Estas conexiones pueden tardar varios minutos en completarse de forma correcta.

Contenido

Antes de iniciar un cambio de zona

- El cambio de zona está deshabilitado de manera predeterminada y se debe habilitar en cada equilibrador de carga de red. Para obtener más información, consulte Habilitación del cambio de zona para el equilibrador de carga de red.
- Puede iniciar un cambio de zona para un equilibrador de carga de red específico solo para una única zona de disponibilidad. No puede comenzar un cambio de zona para varias zonas de disponibilidad.
- AWS elimina de manera 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 utiliza un cambio de zona en el equilibrador de carga de red, la zona de disponibilidad afectada por el cambio de zona también pierde capacidad de destino.
- Durante un cambio de zona en equilibradores de carga de red con el equilibrio de carga entre zonas habilitado, las direcciones IP del equilibrador de carga de zona se eliminan del DNS. Las

conexiones existentes con destinos de la zona de disponibilidad afectada persisten hasta que se cierran de manera orgánica, mientras que las nuevas conexiones dejan de enrutarse a destinos de la zona de disponibilidad afectada.

Para obtener más información, consulte Prácticas recomendadas para cambios de zona en ARC en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon (ARC).

Anulación administrativa por cambio de zona

Los destinos que pertenezcan a un equilibrador de carga de red incluirán el nuevo estado `AdministrativeOverride`, que es independiente del estado `TargetHealth`.

Cuando se inicia un cambio de zona para un equilibrador de carga de red, todos los destinos de la zona de la que se están moviendo se consideran anulados administrativamente. El equilibrador de carga de red deja de enrutar tráfico nuevo hacia los destinos anulados administrativamente. Las conexiones existentes permanecen intactas hasta que se cierran de forma natural.

Los estados posibles de `AdministrativeOverride` son:

unknown

El estado no se puede propagar debido a un error interno

no_override

No existe ninguna anulación activa en el destino actualmente

zonal_shift_active

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

zonal_shift_delegated_to_dns

El estado de cambio de zona de este destino no está disponible a través de `DescribeTargetHealth`, pero se puede consultar directamente mediante la API o la consola de AWS ARC - Zonal Shift.

Habilitación del cambio de zona para el equilibrador de carga de red

El cambio de zona está deshabilitado de manera predeterminada y se debe habilitar en cada equilibrador de carga de red. Esto garantiza que pueda iniciar un cambio de zona únicamente en los

equilibradores de carga de red específicos que desee. Para obtener más información, consulte the section called “Cambio de zona”.

Requisitos previos

Si habilita el equilibrio de carga entre zonas para el equilibrador de carga, cada grupo de destino asociado debe cumplir los siguientes requisitos antes de poder habilitar el cambio de zona:

- El protocolo del grupo de destino debe ser `TCP` o `TLS`.
- El tipo de grupo de destino no debe ser `alb`.
- La terminación de conexiones para destinos en mal estado debe estar desactivada.
- El atributo del grupo de destino `load_balancing.cross_zone.enabled` debe ser `true` o `use_load_balancer_configuration` (valor predeterminado).

Console

Para habilitar el cambio de zona

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 equilibrador de carga de red.
4. En la pestaña Atributos, seleccione Editar.
5. Bajo Configuración de enrutamiento de la zona de disponibilidad, en Integración de cambios de zona de ARC, elija Habilitar.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar el cambio de zona

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

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=zonal_shift.config.enabled,Value=true"
```

CloudFormation

Para habilitar el cambio de zona

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer para incluir el atributo `zonal_shift.config.enabled`.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        -Key: "zonal_shift.config.enabled"
         Value: "true"
```

Inicio de un cambio de zona para el equilibrador de carga de red

El cambio de zona en ARC permite desviar temporalmente el tráfico de los recursos compatibles fuera de una zona de disponibilidad de modo que la aplicación pueda continuar en funcionamiento con normalidad con otras zonas de disponibilidad en una región de AWS.

Requisito previo

Antes de comenzar, verifique que haya habilitado el cambio de zona para el equilibrador de carga.

Console

Este procedimiento explica cómo iniciar un cambio de zona mediante la consola de Amazon EC2. Para conocer los pasos para iniciar un cambio de zona mediante la consola de ARC, consulte Cómo iniciar un cambio de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones (ARC) de Amazon.

Comenzar un cambio de zona

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 equilibrador de carga de red.
4. En la pestaña Integraciones, expanda Controlador de recuperación de aplicaciones de Amazon (ARC) y elija Iniciar 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. Puede actualizar el cambio de zona más adelante para editar el comentario.
8. Seleccione la casilla para confirmar que está al tanto de que iniciar un cambio de zona reduce la capacidad de la aplicación al desviar el tráfico fuera de la zona de disponibilidad.
9. Elija Confirmar.

AWS CLI

Comenzar un cambio de zona

Use el comando start-zonal-shift del Controlador de recuperación de aplicaciones de Amazon (ARC).

```
aws arc-zonal-shift start-zonal-shift \
    --resource-identifier load-balancer-arn \
    --away-from use2-az2 \
    --expires-in 2h \
    --comment "zonal shift due to scheduled maintenance"
```

Actualización de un cambio de zona para el equilibrador de carga de red

Puede actualizar un cambio zonal para establecer un nuevo vencimiento, o bien editar o reemplazar el comentario del cambio zonal.

Console

Este procedimiento explica cómo actualizar un cambio de zona mediante la consola de Amazon EC2. Para conocer los pasos para actualizar un cambio de zona mediante la consola del Controlador de recuperación de aplicaciones (ARC) de Amazon, consulte Cómo actualizar un cambio de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones (ARC) de Amazon.

Actualizar un cambio de zona

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 equilibrador de carga de aplicaciones con un cambio de zona activo.
4. En la pestaña Integraciones, expanda Controlador de recuperación de aplicaciones de Amazon (ARC) y elija Actualizar cambio de zona.

   Esto abre la consola de ARC para continuar con el proceso de actualización.
5. (Opcional) En Establecer vencimiento del cambio de zona, seleccione o introduzca un vencimiento.
6. (Opcional) En Comentario, si lo desea, edite el comentario existente o introduzca un nuevo comentario.
7. Elija Actualizar.

AWS CLI

Actualizar un cambio de zona

Use el comando update-zonal-shift del Controlador de recuperación de aplicaciones de Amazon (ARC).

```
aws arc-zonal-shift update-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE \
    --expires-in 1h \
    --comment "extending zonal shift for scheduled maintenance"
```

Cancelación de un cambio de zona para el equilibrador de carga de red

Puedes cancelar un cambio zonal en cualquier momento antes de que caduque. Puede cancelar los cambios de zona que inicie o los cambios de zona que AWS inicie de un recurso para una ejecución de práctica de cambio automático de zona.

Console

Este procedimiento explica cómo cancelar un cambio de zona mediante la consola de Amazon EC2. Para conocer los pasos para cancelar un cambio de zona mediante la consola del Controlador de recuperación de aplicaciones (ARC) de Amazon, consulte Cómo cancelar un cambio de zona en la Guía para desarrolladores del Controlador de recuperación de aplicaciones (ARC) de Amazon.

Cancelar un cambio de zona

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 equilibrador de carga de red con un cambio de zona activo.
4. En la pestaña Integraciones, en Controlador de recuperación de aplicaciones de Amazon (ARC), elija Cancelar cambio de zona.

   Esto abre la consola de ARC para continuar con el proceso de cancelación.
5. Elija Cancelar cambio de zona.
6. Cuando deba confirmar la selección, haga clic en Confirm (Confirmar).

AWS CLI

Cancelar un cambio de zona

Use el comando cancel-zonal-shift del Controlador de recuperación de aplicaciones de Amazon (ARC).

```
aws arc-zonal-shift cancel-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE
```

Reservas de capacidad para el equilibrador de carga de red

Las reservas de unidades de capacidad del equilibrador de carga (LCU) permiten reservar una capacidad mínima estática para el equilibrador de carga. Los equilibradores de carga de red escalan automáticamente para admitir las cargas de trabajo detectadas y satisfacer las necesidades de capacidad. Cuando se configura una capacidad mínima, el equilibrador de carga puede escalar o desescalar verticalmente en función del tráfico recibido, sin permitir que la capacidad baje por debajo del valor mínimo configurado.

Considere el uso de reservas de LCU en las siguientes situaciones:

- Tiene un evento próximo que generará un pico repentino e inusual de tráfico elevado y desea asegurarse de que el equilibrador de carga pueda admitir ese aumento durante el evento.
- Presenta tráfico impredecible con picos pronunciados debido a la naturaleza de la carga de trabajo durante un periodo corto.
- Está en proceso de configurar el equilibrador de carga para incorporar o migrar los servicios en un momento de inicio específico y necesita comenzar con una capacidad alta, en lugar de esperar a que el escalado automático surta efecto.
- Migra cargas de trabajo entre equilibradores de carga y desea configurar el destino para que coincida con la escala del origen.

Cómo estimar la capacidad que necesita

Al determinar la cantidad de capacidad que debe reservar para el equilibrador de carga, recomendamos realizar pruebas de carga o revisar datos históricos de cargas de trabajo que representen el tráfico esperado. Mediante la consola de Elastic Load Balancing, puede estimar cuánta capacidad necesita reservar en función del tráfico revisado.

Como alternativa, puede consultar la métrica de CloudWatch ProcessedBytes para determinar el nivel adecuado de capacidad. La capacidad del equilibrador de carga se reserva en LCU, donde cada LCU equivale a 2,2 Mbps. Puede utilizar la métrica (ProcessedBytes) (máximo) para ver el rendimiento máximo por minuto del tráfico en el equilibrador de carga y, a continuación, convertir ese rendimiento a LCU mediante la tasa de conversión de 2,2 Mbps = 1 LCU.

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

observa y puede que no representen la carga de trabajo específica. Para obtener más información, consulte Calculadora de reservas de unidades de capacidad del equilibrador de carga.

Regiones admitidas

Esta característica está disponible solo en las siguientes regiones:

- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Estocolmo)

Valores mínimo y máximo para una reserva de LCU

La solicitud de reserva total debe ser de al menos 2750 LCU por zona de disponibilidad. El valor máximo se determina según las cuotas de la cuenta. Para obtener más información, consulte the section called “Unidades de capacidad del equilibrador de carga”.

Solicitud de reserva de unidades de capacidad del equilibrador de carga para el equilibrador de carga de red

Antes de usar una reserva de LCU, revise lo siguiente:

- La reserva de LCU no es compatible con equilibradores de carga de red que utilicen oyentes TLS.
- La reserva de LCU solo admite la reserva de capacidad de rendimiento para equilibradores de carga de red. Al solicitar una reserva de LCU, convierta las necesidades de capacidad de Mbps a LCU según la tasa de conversión de 1 LCU = 2,2 Mbps.
- La capacidad se reserva a nivel regional y se distribuye de manera uniforme entre las zonas de disponibilidad. Confirme que tiene suficientes destinos distribuidos de forma uniforme en cada zona de disponibilidad antes de habilitar la reserva de LCU.

- Las solicitudes de reserva de LCU se atienden por orden de llegada y dependen de la capacidad disponible para una zona en ese momento. La mayoría de las solicitudes se suelen completar en menos de una hora, aunque pueden tardar hasta varias horas.
- Para actualizar una reserva existente, la solicitud anterior debe estar aprovisionada o haber fallado. Puede aumentar la capacidad reservada tantas veces como sea necesario; sin embargo, solo puede reducir la capacidad reservada dos veces por día.
- Se aplicarán cargos por cualquier capacidad reservada o aprovisionada hasta que se termine o se cancele.

Console

Para solicitar una reserva de LCU

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 nombre del equilibrador de carga.
4. En la pestaña Capacidad, elija Editar reserva de LCU.
5. Seleccione Estimación basada en referencias históricas.
6. Seleccione el periodo de referencia para ver el nivel recomendado de LCU reservadas.
7. Si no tiene una carga de trabajo de referencia histórica, puede elegir Estimación manual e introducir la cantidad de LCU que se van a reservar.
8. Seleccione Save.

AWS CLI

Para solicitar una reserva de LCU

Utilice el comando modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --minimum-load-balancer-capacity CapacityUnits=3000
```

CloudFormation

Para solicitar una reserva de LCU

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-alb
      Type: application
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      MinimumLoadBalancerCapacity:
        CapacityUnits: 3000
```

Actualización o cancelación de reservas de unidades de capacidad del equilibrador de carga para el equilibrador de carga de red

Si cambian los patrones de tráfico del equilibrador de carga, puede actualizar o cancelar la reserva de LCU del equilibrador de carga.

Console

Para actualizar o cancelar una reserva de LCU

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 nombre del equilibrador de carga.
4. En la pestaña Capacidad, realice una de las siguientes acciones:
   a. Para actualizar la reserva de LCU, elija Editar reserva de LCU.
   b. Para cancelar la reserva de LCU, elija Cancelar capacidad.

AWS CLI

Para cancelar una reserva de LCU

Utilice el comando modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --reset-capacity-reservation
```

Supervisión de la reserva de unidades de capacidad del equilibrador de carga para el equilibrador de carga de red

Estado de la reserva

Los siguientes son los posibles valores de estado para una reserva de LCU:

- `pending`: indica que la reserva se encuentra en proceso de aprovisionamiento.
- `provisioned`: indica que la capacidad reservada está lista y disponible para su uso.
- `failed`: indica que la solicitud no se puede completar en este momento.
- `rebalancing`: indica que se agregó o eliminó una zona de disponibilidad y que el equilibrador de carga está en proceso de reequilibrar la capacidad.

Utilización de LCU

Para determinar la utilización de LCU reservadas, puede comparar la métrica por minuto `ProcessedBytes` con la métrica por hora `Sum(ReservedLCUs)`. Para convertir bytes por minuto a LCU por hora, utilice la siguiente fórmula: (bytes por minuto) × 8 ÷ 60 ÷ (10^6) ÷ 2,2.

Console

Para ver el estado de una reserva de LCU

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 nombre del equilibrador de carga.
4. En la pestaña Capacidad, puede ver Estado de la reserva y el valor de LCU reservadas.

AWS CLI

Para supervisar el estado de una reserva de LCU

Use el comando describe-capacity-reservation.

```
aws elbv2 describe-capacity-reservation \
    --load-balancer-arn load-balancer-arn
```

Oyentes para los equilibradores de carga de red

Un oyente es un proceso que comprueba las solicitudes de conexión mediante el protocolo y el puerto configurados. Antes de comenzar a utilizar el equilibrador de carga de red, 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 un oyente determinan cómo el equilibrador de carga direcciona las solicitudes a sus destinos registrados, como instancias de EC2.

Contenido

Configuración del oyente

Los oyentes son compatibles con los siguientes protocolos y puertos:

- Protocolos: TCP, TLS, UDP, TCP_UDP, QUIC, TCP_QUIC
- Puertos: 1-65535

Puede utilizar un agente de escucha TLS para trasladar la carga de cifrado y descifrado al balanceador de carga con el fin de que las aplicaciones puedan concentrarse en la lógica de negocio. Si el protocolo del oyente es TLS, debe implementar al menos un certificado de servidor SSL en el oyente. Para obtener más información, consulte Certificados de servidor.

Si se debe asegurar de que los destinos descifren el tráfico de TLS en lugar del equilibrador de carga, puede crear un oyente de TCP en el puerto 443 en lugar de crear un oyente de TLS. Con un oyente de TCP, el equilibrador de carga transfiere el tráfico cifrado a los destinos sin descifrarlo.

Puede usar un oyente QUIC para aceptar tráfico QUIC. El equilibrador de carga de red actúa como un equilibrador de carga de paso directo, de conformidad con RFC 9000. Utilice un oyente QUIC y backends con QUIC habilitado para permitir una migración de conexiones fluida en dispositivos móviles.

Para admitir TCP y UDP en el mismo puerto, cree un agente de escucha TCP_UDP. Los grupos de destino de un agente de escucha TCP_UDP deben utilizar el protocolo TCP_UDP.

Para admitir tanto TCP como QUIC en el mismo puerto, cree un oyente TCP_QUIC. Los grupos de destino de un oyente TCP_QUIC deben usar el protocolo TCP_QUIC.

Un oyente UDP para un equilibrador de carga de doble pila requiere grupos de destino IPv6.

WebSockets solo es compatible con oyentes TCP, TLS, TCP_UDP y TCP_QUIC.

El tráfico QUIC no admite la negociación de versiones. QUIC v1 es la única versión de QUIC compatible.

Todo el tráfico de red enviado a un agente de escucha configurado se clasifica como tráfico deseado. El tráfico de red que no coincide con un agente de escucha configurado se clasifica como tráfico no deseado. Las solicitudes de ICMP distintas del tipo 3 también se consideran tráfico no deseado. Los equilibradores de carga de red eliminan el tráfico no deseado sin reenviarlo a un destino. Los paquetes de datos TCP enviados al puerto de los agentes de escucha configurados que no sean conexiones nuevas ni formen parte de una conexión TCP activa se rechazan con un restablecimiento TCP (RST).

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

Acciones predeterminadas

Al crear un oyente, se especifica una acción predeterminada para el enrutamiento de las solicitudes. La acción predeterminada reenvía las solicitudes a los grupos de destino especificados.

Distribución del tráfico entre varios grupos de destino

Si especifica varios grupos de destino para una acción predeterminada, las solicitudes se distribuyen entre estos grupos de destino en función de sus ponderaciones relativas. Debe especificar una ponderación de 0 a 999 para cada grupo de destino. Un grupo de destino con una ponderación de 0 no recibe tráfico. Después de agregar un grupo de destino o de actualizar las ponderaciones de los grupos de destino, las nuevas conexiones se enrutan según las nuevas ponderaciones de los grupos de destino. Las conexiones existentes no se ven afectadas y continúan hasta que se cierran, como de costumbre.

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 grupo de destino con una ponderación de 10.

Un caso de uso común consiste en migrar el tráfico de un grupo de destino a otro. Esto significa que se incrementa gradualmente la ponderación del nuevo grupo de destino mientras se reduce la ponderación del grupo de destino original hasta llegar a 0. Si actualiza la ponderación de un grupo de destino a 0, después de un breve periodo, no recibe nuevas conexiones y las conexiones existentes se cierran.

Sesiones persistentes y grupos de destinos ponderados

Las acciones de reenvío en los oyentes pueden especificar si se habilita la persistencia de grupos de destino. Cuando se habilita, la persistencia de grupos de destino hace que las conexiones posteriores desde la misma dirección IP de origen prefieran el grupo de destino seleccionado previamente.

Consideraciones

- Para oyentes TLS, no se pueden agregar simultáneamente grupos de destino TCP y grupos de destino TLS a la regla del oyente. Todos los grupos de destino deben usar el mismo protocolo.
- Para oyentes TLS, la persistencia de grupos de destino no es compatible.
- En el caso de los equilibradores de carga de doble pila, no se pueden agregar simultáneamente grupos de destino IPv4 y grupos de destino IPv6 a la misma acción predeterminada. Todos los grupos de destino en la acción predeterminada deben usar el mismo tipo de dirección IP.
- En el caso de los oyentes, si una acción de reenvío contiene varios grupos de destino y alguno de ellos tiene la persistencia habilitada, la acción de reenvío también debe tener habilitada la persistencia de grupos de destino.

Atributos del oyente

A continuación se indican los atributos del oyente de los equilibradores de carga de red:

`tcp.idle_timeout.seconds`

Valor del tiempo de inactividad de TCP, en segundos. El rango válido es de 60 a 6000 segundos. El valor predeterminado es de 350 segundos.

Para obtener más información, consulte Actualización del tiempo de inactividad.

Oyentes seguros

Para utilizar un agente de escucha TLS, debe implementar al menos un certificado de servidor en el balanceador de carga. El balanceador 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. Tenga en cuenta que si necesita transferir tráfico cifrado a los destinos sin que el equilibrador de carga lo descifre, debe crear un oyente de TCP en el puerto 443 en lugar de crear un oyente de TLS. El equilibrador de carga transfiere la solicitud al destino tal cual, sin descifrarla.

Elastic Load Balancing utiliza una configuración de negociación de TLS, lo que se conoce como política de seguridad, para negociar las conexiones de TLS 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. El primer cifrado de la lista del servidor que coincide con uno de los cifrados del cliente se selecciona para la conexión segura.

Los equilibradores de carga de red no admiten la autenticación TLS mutua (mTLS). En el caso de la compatibilidad con mTLS, cree un oyente de TCP en lugar de uno de TLS. El equilibrador de carga transmite la solicitud tal cual, de modo que puede implementar mTLS en el destino.

Los equilibradores de carga de red admiten la reanudación de TLS mediante PSK para TLS 1.3 y tickets de sesión para TLS 1.2 y versiones anteriores. No se admiten las reanudaciones con ID

de sesión ni los casos en los que se configuran varios certificados en el oyente mediante SNI. La característica de datos 0-RTT y la extensión early_data no están implementadas.

Para ver demostraciones relacionadas, consulte la Compatibilidad con TLS en el equilibrador de carga de red y la Compatibilidad con SNI en el equilibrador de carga de red.

Políticas de ALPN

La negociación de protocolo de capa de aplicación (ALPN) es una extensión TLS que se envía en los mensajes de saludo iniciales de TLS. ALPN permite a la capa de aplicación negociar qué protocolos deben utilizarse a través de una conexión segura, como HTTP/1 y HTTP/2.

Cuando el cliente inicia una conexión de ALPN, el balanceador de carga compara la lista de preferencias de ALPN del cliente con su política de ALPN. Si el cliente admite un protocolo de la política de ALPN, el balanceador de carga establece la conexión en función de la lista de preferencias de la política de ALPN. De lo contrario, el balanceador de carga no utiliza ALPN.

Políticas de ALPN admitidas

Las siguientes son las políticas de ALPN admitidas:

`HTTP1Only`

Negocian solo HTTP/1.*. La lista de preferencias de ALPN es http/1.1, http/1.0.

`HTTP2Only`

Negocian solo HTTP/2. La lista de preferencias de ALPN es h2.

`HTTP2Optional`

Prefieren HTTP/1.* sobre HTTP/2 (que puede ser útil para pruebas HTTP/2). La lista de preferencias de ALPN es http/1.1, http/1.0, h2.

`HTTP2Preferred`

Prefieren HTTP/2 sobre HTTP/1.*. La lista de preferencias de ALPN es h2, http/1.1, http/1.0.

`None`

No negocian ALPN. Esta es la opción predeterminada.

Habilitar conexiones de ALPN

Puede habilitar conexiones de ALPN cuando cree o modifique un agente de escucha TLS. Para obtener más información, consulte Añadir un agente de escucha y Actualizar la política de ALPN.

Crear un oyente para el equilibrador de carga de red

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

Requisitos previos

- Debe especificar un grupo de destino para la acción predeterminada. Para obtener más información, consulte Para crear un grupo de destino para el equilibrador de carga de red.
- Debe especificar un certificado SSL para un oyente de TLS. El equilibrador de carga usará el certificado para terminar la conexión y descifrar las solicitudes de los clientes antes de direccionarlas a los destinos. Para obtener más información, consulte Certificados de servidor del equilibrador de carga de red.
- No puede usar un grupo de destino IPv4 con un oyente UDP para un equilibrador de carga `dualstack`.
- Los oyentes QUIC y TCP_QUIC no están permitidos en equilibradores de carga `dualstack` o equilibradores de carga con grupos de seguridad asociados.
- Los oyentes QUIC y TCP_QUIC no están permitidos en equilibradores de carga con grupos de seguridad asociados.
- Solo se permite un oyente QUIC o TCP_QUIC en un equilibrador de carga de red en un momento dado.
- Los oyentes QUIC y TCP_QUIC no están permitidos en un equilibrador de carga de red que tenga oyentes UDP o TCP_UDP.

Añadir un agente de escucha

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.

Console

Para agregar un agente de escucha

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 de Oyentes, elija Agregar oyente.
5. Para el campo Protocolo, seleccione TCP, UDP, TCP_UDP, TLS, QUIC o TCP_QUIC. Deje el puerto predeterminado o especifique otro.
6. En Acción predeterminada, seleccione un grupo de destino al que reenviar el tráfico.

   Para agregar otro grupo de destino, elija Agregar grupo de destino y actualice las ponderaciones según sea necesario.

   Si no tiene un grupo de destino que se ajuste a sus necesidades, seleccione Crear grupo de destino para crear uno ahora. Para obtener más información, consulte Creación de un grupo de destino..
7. [Agentes de escucha TLS] En Security policy (Política de seguridad), le recomendamos que mantenga la política de seguridad predeterminada.
8. [Oyentes TLS] En Certificado de servidor SSL/TLS predeterminado, seleccione el certificado predeterminado. Puede seleccionar el certificado de uno de los siguientes orígenes:

   - Si creó o importó un certificado mediante AWS Certificate Manager, seleccione Desde ACM y, a continuación, elija el certificado en Certificado (desde ACM).
   - Si importó un certificado mediante IAM, seleccione Desde IAM y, a continuación, elija el certificado en Certificado (desde IAM).
   - Si dispone de un certificado, seleccione Importar certificado. Seleccione Importar a ACM o Importar a IAM. En Clave privada del certificado, copie y pegue el contenido del archivo de clave privada (codificado en PEM). En Cuerpo del certificado, copie y pegue el contenido del archivo del certificado de clave pública (codificado en PEM). En Cadena del certificado, copie y pegue el contenido del archivo de la cadena del certificado (codificado en PEM), a menos que use un certificado autofirmado y no sea importante que los navegadores acepten implícitamente el certificado.

9. [Agentes de escucha TLS] Para la política de ALPN, elija una política para habilitar ALPN o elija None (Ninguna) para deshabilitar ALPN. Para obtener más información, consulte Políticas de ALPN.
10. (Opcional) Para agregar etiquetas, expanda Etiquetas del oyente. Seleccione Agregar nueva etiqueta e ingrese la clave y el valor de la etiqueta.
11. Elija Agregar.
12. [Oyentes TLS] Para agregar certificados a la lista opcional de certificados, consulte Añadir certificados a la lista de certificados.

AWS CLI

Creación de un grupo de destino

Si no tiene un grupo de destino que pueda usar para la acción predeterminada, use el comando create-target-group para crear uno ahora. Para ver ejemplos, consulte Creación de un grupo de destino..

Para agregar un oyente TCP

Use el comando create-listener, especificando el protocolo TCP.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Para agregar un oyente TCP con varios grupos de destino

Use el comando create-listener, especificando el protocolo TCP, los grupos de destino y las ponderaciones.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
```

```
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
            ]
        }
    }]'
```

Para agregar un oyente TLS

Use el comando create-listener, especificando el protocolo TLS.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TLS \
    --port 443 \
    --certificates CertificateArn=certificate-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Para agregar un oyente UDP

Use el comando create-listener, especificando el protocolo UDP.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol UDP \
    --port 53 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Para agregar un oyente QUIC

Use el comando create-listener, especificando el protocolo QUIC.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol QUIC \
    --port 443 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Para agregar un oyente TCP

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::Listener mediante el protocolo TCP.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Para agregar un oyente TCP con varios grupos de destino

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::Listener mediante el protocolo TCP.

```
Resources:
    myTCPListener:
        Type: 'AWS::ElasticLoadBalancingV2::Listener'
        Properties:
        LoadBalancerArn: !Ref myLoadBalancer
        Protocol: TCP
        Port: 80
        DefaultActions:
            - Type: forward
            ForwardConfig:
                TargetGroups:
                - TargetGroupArn: !Ref myTargetGroup1,
                    Weight: 10
                - TargetGroupArn: !Ref myTargetGroup2,
                    Weight: 30
            TargetGroupStickinessConfig:
                Enabled: true
```

Para agregar un oyente TLS

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::Listener mediante el protocolo TLS.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
```

```
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Para agregar un oyente UDP

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::Listener mediante el protocolo UDP.

```
Resources:
  myUDPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: UDP
      Port: 53
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Para agregar un oyente QUIC

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::Listener mediante el protocolo QUIC.

```
Resources:
  myQUICListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: QUIC
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Certificados de servidor del equilibrador de carga de red

Cuando se crea un oyente seguro para el equilibrador de carga de red, se debe implementar al menos un certificado en el equilibrador de carga. El balanceador de carga requiere certificados X.509 (certificado de servidor). 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 de los equilibradores de carga. 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.

Si lo desea, también puede utilizar las herramientas de TLS para crear una solicitud de firma de certificado (CSR), obtener la CSR firmada por una CA para generar el certificado e importar el certificado en ACM o cargarlo en AWS Identity and Access Management (IAM). Para obtener más información, consulte Importación de certificados en la Guía del usuario de AWS Certificate Manager o Trabajo con certificados de servidor en la Guía del usuario de IAM.

Algoritmos de clave admitidos

- RSA de 1024 bits

- RSA de 2048 bits
- RSA de 3072 bits
- ECDSA de 256 bits
- ECDSA de 384 bits
- ECDSA de 521 bits

Certificado predeterminado

Al crear un oyente TLS, debe especificar al menos un certificado. Este certificado se conoce como certificado predeterminado. Puede sustituir el certificado predeterminado después de crear el agente de escucha TLS. 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 agente de escucha TLS, 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 AWS Certificate Manager e implementados en el equilibrador de carga se pueden renovar automáticamente. ACM intenta renovar los certificados antes de que venzan. Para obtener más información, consulte Renovación administrada en la Guía del usuario de AWS Certificate Manager.
- Si el certificado se importó en ACM, deberá monitorear la fecha de vencimiento del certificado y renovarlo antes de que venza. Para obtener más información, consulte Importación de certificados en la Guía del usuario de AWS Certificate Manager.
- Si importa un certificado en IAM, debe crear un nuevo certificado, importar el nuevo certificado en ACM o IAM, añadir el nuevo certificado al equilibrador de carga y eliminar el certificado caducado del equilibrador de carga.

Políticas de seguridad para el equilibrador de carga de red

Al crear un agente de escucha TLS, debe seleccionar una política de seguridad. Una política de seguridad determina qué cifrados y protocolos se admiten durante las negociaciones SSL entre el equilibrador de carga y los clientes. Puede actualizar la política de seguridad del equilibrador de carga si cambian sus requisitos, o cuando publicamos una nueva política de seguridad. Para obtener más información, consulte Actualizar la política de seguridad.

Consideraciones

- Un oyente TLS requiere una política de seguridad. Si no especifica una política de seguridad al crear el oyente, se usará la política de seguridad predeterminada. La política de seguridad predeterminada depende de cómo haya creado el oyente TLS:
  - Consola: la política de seguridad predeterminada es `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`.
  - Otros métodos (por ejemplo, la AWS CLI, AWS CloudFormation y AWS CDK): la política de seguridad predeterminada es `ELBSecurityPolicy-2016-08`.
- Puede seleccionar la política de seguridad que se utiliza para las conexiones frontend, pero no para las conexiones backend. La política de seguridad para las conexiones con el backend depende de la política de seguridad del oyente:
  - Si el oyente TLS usa una política de seguridad TLS 1.3, las conexiones de backend usan la política `ELBSecurityPolicy-TLS13-1-0-2021-06`.
  - Si el oyente TLS no usa una política de seguridad TLS 1.3, las conexiones de backend usan la política `ELBSecurityPolicy-2016-08`.
- Puede habilitar los registros de acceso para obtener información sobre las solicitudes TLS enviadas al equilibrador de carga de red, analizar patrones de tráfico TLS, administrar actualizaciones de políticas de seguridad y solucionar problemas. Habilite el registro de acceso del equilibrador de carga y examine las entradas del registro de acceso correspondientes. Para obtener más información, consulte Registros de acceso y Consultas de ejemplo del equilibrador de carga de red.
- Puede restringir las políticas de seguridad que están disponibles para los usuarios en todas las Cuentas de AWS y AWS Organizations mediante las claves de condición de Elastic Load Balancing en las políticas de control de servicios (SCP) e IAM, respectivamente. Para obtener más información, consulte Políticas de control de servicios (SCP) en la Guía del usuario de AWS Organizations.
- Las políticas que admiten únicamente TLS 1.3 son compatibles con el secreto directo (FS). Las políticas que admiten TLS 1.3 y TLS 1.2 y que incluyen únicamente cifrados de la forma TLS_* y ECDHE_* también proporcionan secreto directo (FS).
- Los equilibradores de carga de red admiten la extensión Extended Master Secret (EMS) para TLS 1.2.

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

Políticas de seguridad

Políticas de seguridad de TLS

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

Las políticas que admiten únicamente TLS 1.3 son compatibles con el secreto directo (FS). Las políticas que admiten TLS 1.3 y TLS 1.2 y que incluyen únicamente cifrados de la forma TLS_* y ECDHE_* también proporcionan secreto directo (FS).

Contenido

Protocolos por política

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

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

Cifrados por política

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

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-3-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256
ELBSecurityPolicy-TLS13-1-2-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-Res-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256

Política de seguridad	Cifrados
	• ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-1-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-0-2021-06	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS-1-2-Ext-2018-06	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS-1-2-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS-1-1-2017-01	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-2016-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-2015-05	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES256-SHA • ECDHE-RSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Políticas por cifrado

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

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: TLS_AES_128_GCM_SHA256 IANA: TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-2-2021-06	1301

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
	• ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06	
OpenSSL: TLS_AES_256_GCM_SHA384 IANA: TLS_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06	1302

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: TLS_CHACHA20_POLY1305_SHA256 IANA: TLS_CHACHA20_POLY1305_SHA256	• ELBSecurityPolicy-TLS13-1-3-2021-06 • ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06	1303

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02b

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-RSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02f

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES128-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c023

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL – ECDHE-RSA-AES128-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c027
OpenSSL: ECDHE-ECDSA-AES128-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c009

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-RSA-AES128-SHA IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c013
OpenSSL: ECDHE-ECDSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c02c

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-RSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Res-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c030

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES256-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c024

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-RSA-AES256-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c028
OpenSSL: ECDHE-ECDSA-AES256-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c00a

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-RSA-AES256-SHA IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	c014
OpenSSL: AES128-GCM-SHA256 IANA: TLS_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	9c

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: AES128-SHA256 IANA: TLS_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	3c
OpenSSL: AES128-SHA IANA: TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	2f

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: AES256-GCM-SHA384 IANA: TLS_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	9d
OpenSSL: AES256-SHA256 IANA: TLS_RSA_WITH_AES_256_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-2-2017-01 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	3d

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: AES256-SHA IANA: TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06 • ELBSecurityPolicy-TLS13-1-1-2021-06 • ELBSecurityPolicy-TLS13-1-0-2021-06 • ELBSecurityPolicy-TLS-1-2-Ext-2018-06 • ELBSecurityPolicy-TLS-1-1-2017-01 • ELBSecurityPolicy-2016-08	35

Políticas de seguridad FIPS

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

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

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

Contenido

Protocolos por política

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

Políticas de seguridad	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	Sí	No	No	No
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04	Sí	Sí	No	No
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04	Sí	Sí	No	No
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04	Sí	Sí	No	No
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04	Sí	Sí	No	No
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04	Sí	Sí	No	No
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	Sí	Sí	Sí	No
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	Sí	Sí	Sí	Sí

Cifrados por política

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

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384
ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384

Política de seguridad	Cifrados
	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA
ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • AES128-GCM-SHA256 • AES128-SHA256 • AES256-GCM-SHA384 • AES256-SHA256

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA • AES128-GCM-SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM-SHA384 • AES256-SHA256 • AES256-SHA

Políticas por cifrado

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

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04	1301

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
IANA: TLS_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	
OpenSSL: TLS_AES_256_GCM_SHA384 IANA: TLS_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	1302

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL – ECDHE-ECDSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c02b
OpenSSL: ECDHE-RSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c02f

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES128-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c023
OpenSSL – ECDHE-RSA-AES128-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c027

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES128-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c009
OpenSSL: ECDHE-RSA-AES128-SHA IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c013

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c02c
OpenSSL: ECDHE-RSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c030

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES256-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c024
OpenSSL: ECDHE-RSA-AES256-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c028

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-ECDSA-AES256-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c00a
OpenSSL: ECDHE-RSA-AES256-SHA IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	c014
OpenSSL: AES128-GCM-SHA256 IANA: TLS_RSA_WITH_AES_128_GCM_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	9c

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: AES128-SHA256 IANA: TLS_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	3c
OpenSSL: AES128-SHA IANA: TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	2f
OpenSSL: AES256-GCM-SHA384 IANA: TLS_RSA_WITH_AES_256_GCM_SHA384	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	9d

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: AES256-SHA256 IANA: TLS_RSA_WITH_AES_256_CBC_SHA256	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	3d
OpenSSL: AES256-SHA IANA: TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04 • ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04	35

Políticas de seguridad FS admitidas

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

Las políticas de esta sección son compatibles con el secreto directo (FS) y “FS” está incluido en sus nombres. Sin embargo, estas no son las únicas políticas que admiten secreto directo (FS). Las políticas que admiten únicamente TLS 1.3 son compatibles con el secreto directo (FS). Las políticas que admiten TLS 1.3 y TLS 1.2 y que incluyen únicamente cifrados de la forma TLS_* y ECDHE_* también proporcionan secreto directo (FS).

Contenido

- Políticas por cifrado

Protocolos por política

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

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

Cifrados por política

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

Política de seguridad	Cifrados
ELBSecurityPolicy-FS-1-2-Res-2020-10	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384
ELBSecurityPolicy-FS-1-2-Res-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256

Política de seguridad	Cifrados
	• ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384
ELBSecurityPolicy-FS-1-2-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

Política de seguridad	Cifrados
ELBSecurityPolicy-FS-1-1-2019-08	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA
ELBSecurityPolicy-FS-2018-06	• ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 • ECDHE-ECDSA-AES128-SHA • ECDHE-RSA-AES128-SHA • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA • ECDHE-ECDSA-AES256-SHA

Políticas por cifrado

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

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL – ECDHE-ECDSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• 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	c02b
OpenSSL: ECDHE-RSA-AES128-GCM-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• 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	c02f
OpenSSL: ECDHE-ECDSA-AES128-SHA256 IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c023
OpenSSL – ECDHE-RSA-AES128-SHA256 IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c027
OpenSSL: ECDHE-ECDSA-AES128-SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c009

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
IANA: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		
OpenSSL: ECDHE-RSA-AES128-SHA IANA: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c013
OpenSSL: ECDHE-ECDSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• 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	c02c
OpenSSL: ECDHE-RSA-AES256-GCM-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• 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	c030
OpenSSL: ECDHE-ECDSA-AES256-SHA384 IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c024

Nombre del cifrado	Políticas de seguridad	Conjunto de cifrado
OpenSSL: ECDHE-RSA-AES256-SHA384 IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• ELBSecurityPolicy-FS-1-2-Res-2019-08 • ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c028
OpenSSL: ECDHE-ECDSA-AES256-SHA IANA: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c00a
OpenSSL: ECDHE-RSA-AES256-SHA IANA: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolicy-FS-1-2-2019-08 • ELBSecurityPolicy-FS-1-1-2019-08 • ELBSecurityPolicy-FS-2018-06	c014

Actualizar un oyente para el equilibrador de carga de red

Puede actualizar el protocolo del oyente, el puerto del oyente o el grupo de destino que recibe el tráfico de la acción de reenvío. La acción predeterminada, también conocida como regla predeterminada, reenvía las solicitudes al grupo de destino seleccionado.

Si cambia el protocolo de TCP, UDP o QUIC a TLS, debe especificar una política de seguridad y un certificado de servidor. Si cambia el protocolo de TLS a TCP, UDP o QUIC, se eliminan la política de seguridad y el certificado de servidor.

Cuando se actualiza el grupo de destino de la acción predeterminada de un oyente TCP, TLS o QUIC, las nuevas conexiones se enrutan al grupo de destino configurado recientemente. Sin embargo, esto no afecta a conexiones activas que se hayan creado antes de este cambio. Estas conexiones activas permanecen asociadas al destino del grupo de destino original durante un máximo de una hora si se envía tráfico, o hasta que se agote el tiempo de espera de inactividad si no se envía tráfico, lo que ocurra primero. El parámetro `Connection termination on deregistration` no se aplica al actualizar el oyente, sino al anular el registro de los destinos.

No se permiten actualizaciones de puerto para oyentes QUIC o TCP_QUIC. Para actualizar el puerto de los oyentes que manejan tráfico QUIC, el oyente se debe eliminar y volver a crear con el nuevo puerto.

Console

Para actualizar un oyente

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 su página de detalles.
4. En la pestaña de Oyentes, elija el texto de la columna Protocol:Port para abrir la página de detalles del oyente.
5. Seleccione Acciones y, a continuación, Editar oyente.
6. Actualice los valores según sea necesario.
   - (Opcional) Cambie el Protocolo.
   - (Opcional) Cambie el Puerto.
   - (Opcional) Seleccione grupos de destino diferentes para Acción predeterminada.
   - (Opcional) Para agregar otro grupo de destino, seleccione Agregar grupo de destino y actualice las ponderaciones según sea necesario.
   - (Opcional) Para eliminar un grupo de destino, seleccione Eliminar.
7. (Opcional) Agregue, actualice o elimine etiquetas según sea necesario.
8. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar la acción predeterminada

Use el comando modify-listener para cambiar el grupo de destino.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions Type=forward,TargetGroupArn=new-target-group-arn
```

El siguiente ejemplo actualiza un oyente con varios grupos de destino.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions '[{
        "Type":"forward",
        "ForwardConfig":{
            "TargetGroups":[
                {"TargetGroupArn":"target-group-1-arn","Weight":10},
                {"TargetGroupArn":"target-group-2-arn","Weight":30}
            ]
        }
    }]'
```

Para agregar etiquetas de

Utilice el comando add-tags. En el siguiente ejemplo, se agregan dos etiquetas.

```
aws elbv2 add-tags \
    --resource-arns listener-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Para eliminar etiquetas

Utilice el comando remove-tags. En el siguiente ejemplo, se eliminan las etiquetas con las claves especificadas.

```
aws elbv2 remove-tags \
    --resource-arns listener-arn \
    --tag-keys project department
```

CloudFormation

Para actualizar la acción predeterminada

Actualice el recurso AWS::ElasticLoadBalancingV2::Listener para incluir el nuevo grupo de destino.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
```

```
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref newTargetGroup
```

Como alternativa, para distribuir el tráfico entre varios grupos de destino, defina `DefaultActions` como se indica a continuación.

```
DefaultActions:
    - Type: forward
    ForwardConfig:
        TargetGroups:
        - TargetGroupArn: !Ref TargetGroup1
            Weight: 10
        - TargetGroupArn: !Ref TargetGroup2
            Weight: 30
```

Para agregar etiquetas de

Actualice el recurso AWS::ElasticLoadBalancingV2::Listener para incluir la propiedad Etiquetas.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Actualización del tiempo de inactividad de TCP del oyente del equilibrador de carga de red

Para cada solicitud de TCP realizada a través de un equilibrador de carga de red, se realiza un seguimiento del estado de esa conexión. Si transcurre el tiempo de inactividad sin que el cliente ni el destinatario envíen datos a través de la conexión, esta se cierra.

Consideraciones

- El valor predeterminado del tiempo de espera de inactividad para los flujos TCP es de 350 segundos.
- El tiempo de espera de inactividad de la conexión para los oyentes TLS es de 350 segundos y no se puede modificar.

Console

Para actualizar el tiempo de espera de inactividad de TCP

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 del equilibrador de carga de red.
4. En la pestaña Oyentes, seleccione la casilla del oyente TCP y, a continuación, elija Acciones y Ver detalles del oyente.
5. En la página de detalles del oyente, en la pestaña Atributos, seleccione Editar. Si el oyente utiliza un protocolo distinto de TCP, esta pestaña no está disponible.
6. Introduzca un valor para Tiempo de espera de inactividad de TCP entre 60 y 6000 segundos.
7. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar el tiempo de espera de inactividad de TCP

Utilice el comando modify-listener-attributes con el atributo `tcp.idle_timeout.seconds`.

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

```
    --listener-arn listener-arn \
    --attributes Key=tcp.idle_timeout.seconds,Value=500
```

A continuación, se muestra un ejemplo del resultado.

```
{
    "Attributes": [
        {
            "Key": "tcp.idle_timeout.seconds",
            "Value": "500"
        }
    ]
}
```

CloudFormation

Para actualizar el tiempo de espera de inactividad de TCP

Actualice el recurso AWS::ElasticLoadBalancingV2::Listener para incluir el atributo del oyente `tcp.idle_timeout.seconds`.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      ListenerAttributes:
        - Key: "tcp.idle_timeout.seconds"
          Value: "500"
```

Actualizar un oyente de TLS para el equilibrador de carga de red

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

Tareas

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

Reemplazar el certificado predeterminado

Puede reemplazar el certificado predeterminado del oyente TLS según sea necesario. Para obtener más información, consulte Certificado predeterminado.

Console

Para reemplazar el certificado predeterminado

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 de Oyentes, elija el texto de la columna Protocol:Port 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. (Opcional) De forma predeterminada, seleccionamos Agregar certificado predeterminado anterior a la lista de certificados del oyente. Recomendamos mantener esta opción seleccionada, a menos que actualmente no tenga certificados de oyente para SNI y dependa de la reanudación de sesión TLS.
8. Seleccione Guardar como predeterminado.

AWS CLI

Para reemplazar el certificado predeterminado

Utilice el comando modify-oyente.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --certificates CertificateArn=new-default-certificate-arn
```

CloudFormation

Para reemplazar el certificado predeterminado

Actualice el recurso AWS::ElasticLoadBalancingV2::Listener con el nuevo certificado predeterminado.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "new-default-certificate-arn"
```

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 agente de escucha TLS, la lista de certificados está vacía. Puede agregar el certificado predeterminado a la lista de certificados para garantizar que este certificado se utilice con el protocolo SNI, incluso si se reemplaza como certificado predeterminado. Para obtener más información, consulte Lista de certificados.

Console

Para agregar certificados a la lista de certificados

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 su página de detalles.

4. En la pestaña de Oyentes, elija el texto de la columna Protocol:Port para abrir la página de detalles del oyente.
5. Seleccione la pestaña Certificados.
6. Para agregar el certificado predeterminado a la lista, seleccione Agregar predeterminado a la lista.
7. Para agregar a la lista certificados que no sean predeterminados, haga lo siguiente:

   a. Seleccione Agregar certificado.

   b. Para agregar certificados que ya administra ACM o IAM, seleccione las casillas de verificación de los certificados y elija Incluir como pendiente a continuación.

   c. Para agregar un certificado que no sea administrado por ACM o IAM, seleccione Importar certificado, complete el formulario y elija Importar.

   d. Elija Agregar certificados pendientes.

AWS CLI

Para agregar certificados a la lista de certificados

Utilice el comando add-oyente-certificates.

```
aws elbv2 add-listener-certificates \
    --listener-arn listener-arn \
    --certificates \
        CertificateArn=certificate-arn-1 \
        CertificateArn=certificate-arn-2 \
        CertificateArn=certificate-arn-3
```

CloudFormation

Para agregar certificados a la lista de certificados

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::ListenerCertificate.

```
Resources:
  myCertificateList:
    Type: 'AWS::ElasticLoadBalancingV2::ListenerCertificate'
    Properties:
      ListenerArn: !Ref myTLSListener
```

```
      Certificates:
        - CertificateArn: "certificate-arn-1"
        - CertificateArn: "certificate-arn-2"
        - CertificateArn: "certificate-arn-3"

  myTLSListener:
    Type: AWS::ElasticLoadBalancingV2::Listener
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLSS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn-1"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Quitar certificados de la lista de certificados

Puede quitar certificados de la lista de certificados de un agente de escucha TLS mediante el siguiente procedimiento. Después de eliminar un certificado, el oyente ya no puede crear conexiones con ese certificado. Para asegurarse de que los clientes no se vean afectados, agregue un nuevo certificado a la lista y confirme que las conexiones funcionan antes de eliminar un certificado de la lista.

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

Console

Para eliminar certificados de la lista de certificados

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 su página de detalles.
4. En la pestaña de Oyentes, elija 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.

AWS CLI

Para eliminar certificados de la lista de certificados

Utilice el comando remove-oyente-certificates.

```
aws elbv2 remove-listener-certificates \
    --listener-arn listener-arn \
    --certificates CertificateArn=certificate-arn
```

Actualizar la política de seguridad

Cuando cree un agente de escucha TLS, puede seleccionar la política de seguridad que mejor se ajuste a sus necesidades. Cuando se agrega una política de seguridad nueva, puede actualizar el oyente de TLS para que la utilice. Los equilibradores de carga de red no admiten las políticas de seguridad personalizadas. Para obtener más información, consulte Políticas de seguridad para el equilibrador de carga de red.

Actualizar la política de seguridad puede ocasionar interrupciones si el equilibrador de carga maneja un alto volumen de tráfico. Para reducir la posibilidad de interrupciones cuando el equilibrador de carga maneja un alto volumen de tráfico, cree un equilibrador de carga adicional para ayudar a manejar el tráfico o solicite una reserva de LCU.

Console

Para actualizar la política de seguridad

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 su página de detalles.
4. En la pestaña de Oyentes, elija el texto de la columna Protocol:Port para abrir la página de detalles del oyente.
5. Seleccione Acciones y, a continuación, Editar oyente.
6. En la sección Configuración segura del oyente, en Política de seguridad, elija una nueva política de seguridad.

7. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar la política de seguridad

Utilice el comando modify-oyente.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06
```

CloudFormation

Para actualizar la política de seguridad

Actualice el recurso AWS::ElasticLoadBalancingV2::Listener con la nueva política de seguridad.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "default-certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Actualizar la política de ALPN

Puede actualizar la política ALPN del oyente TLS según sea necesario. Para obtener más información, consulte Políticas de ALPN.

Console

Para actualizar la política ALPN

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 su página de detalles.
4. En la pestaña de Oyentes, elija el texto de la columna Protocol:Port para abrir la página de detalles del oyente.
5. Seleccione Acciones y, a continuación, Editar oyente.
6. En la sección Configuración segura del oyente, en Política ALPN, seleccione una política para habilitar ALPN o elija Ninguna para desactivar ALPN.
7. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar la política ALPN

Utilice el comando modify-oyente.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --alpn-policy HTTP2Preferred
```

CloudFormation

Para actualizar la política ALPN

Actualice el recurso AWS::ElasticLoadBalancingV2::Listener para incluir la política ALPN.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      AlpnPolicy:
```

```
        - HTTP2Preferred
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Eliminar un oyente de para el equilibrador de carga de red

Antes de eliminar un oyente, considere el impacto en la aplicación:

- [Oyentes TCP y TLS] El equilibrador de carga deja de aceptar inmediatamente nuevas conexiones en el oyente. Cualquier establecimiento de comunicación TLS en curso podría fallar. Las conexiones existentes permanecen abiertas hasta que se cierran de forma natural o expiran por tiempo de espera. Las solicitudes en curso en las conexiones existentes se completan correctamente.
- [Oyentes UDP y QUIC] Es posible que los paquetes en tránsito no lleguen a su destino.

Console

Para eliminar un oyente

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 la casilla de verificación de equilibrador de carga.
4. En la pestaña de Oyentes, seleccione la casilla de verificación del oyente y, a continuación, elija Acciones, Eliminar oyente.
5. Cuando se le pida confirmación, ingrese **`confirm`** y elija Eliminar.

AWS CLI

Para eliminar un oyente

Utilice el comando delete-listener.

```
aws elbv2 delete-listener \
    --listener-arn listener-arn
```

Grupos de destino para los equilibradores de carga de red

Cada grupo de destino se utiliza para direccionar solicitudes a uno o varios destinos registrados. Cuando se crea un agente de escucha, especifica un grupo de destino para su acción predeterminada. El tráfico se reenvía al grupo de destino especificado en la regla del agente de escucha. Puede crear grupos de destino diferentes para los distintos tipos de solicitudes. Por ejemplo, puede crear un grupo de destino para las solicitudes generales y otros grupos de destino para las solicitudes destinadas a los microservicios de la aplicación. Para obtener más información, consulte Componentes del equilibrador de carga de red.

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. Para obtener más información, consulte Comprobaciones de estado de grupos de destino del equilibrador de carga de red.

Contenido

- Eliminación de un grupo de destino del equilibrador de carga de red

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 de los equilibradores de carga de red admiten los siguientes protocolos y puertos:

- Protocolos: TCP, TLS, UDP, TCP_UDP, QUIC, TCP_QUIC
- Puertos: 1-65535

Si un grupo de destino está configurado con el protocolo TLS, el balanceador 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. Dado que el equilibrador de carga se encuentra en una nube privada virtual (VPC), el tráfico entre el equilibrador de carga y los destinos se autentica en el nivel de paquete, por lo que no corre el riesgo de sufrir ataques man-in-the-middle ni de suplantación, incluso aunque los certificados de los destinos no sean válidos.

En la tabla siguiente se resumen las combinaciones admitidas de configuración de grupo de destino y protocolo de agente de escucha.

Protocolo del agente de escucha	Protocolo del grupo de destino	Tipo de grupo de destino	Protocolo de comprobación de estado
TCP	TCP | TCP_UDP | TCP_QUIC	instance | ip	HTTP | HTTPS | TCP
TCP	TCP	alb	HTTP | HTTPS
TLS	TCP | TLS	instance | ip	HTTP | HTTPS | TCP
UDP	UDP | TCP_UDP	instance | ip	HTTP | HTTPS | TCP

Protocolo del agente de escucha	Protocolo del grupo de destino	Tipo de grupo de destino	Protocolo de comprobación de estado
TCP_UDP	TCP_UDP	instance | ip	HTTP | HTTPS | TCP
QUIC	QUIC | TCP_QUIC	instance | ip	HTTP | HTTPS | TCP
TCP_QUIC	TCP_QUIC	instance | ip	HTTP | HTTPS | TCP

Tipo de destino

Al crear un grupo de destino, debe especificar su tipo de destino, que determina cómo especificará sus destinos. 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 se especifican por dirección IP.

`alb`

El destino es un equilibrador de carga de aplicación.

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

- Las subredes de la VPC del grupo de destinos
- 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 de CIDR compatibles le permiten registrar los siguientes destinos en un grupo de destino:

- Los recursos de AWS que se pueden direccionar mediante una dirección IP y un puerto (por ejemplo, bases de datos).
- Recursos en las instalaciones vinculados a AWS mediante Direct Connect o a una conexión de VPN Site-to-Site.

Cuando la preservación de la IP del cliente está deshabilitada para los grupos de destino, el equilibrador de carga puede admitir aproximadamente 55 000 conexiones por minuto para cada combinación de dirección IP del equilibrador de carga de red y destino único (dirección IP y puerto). Si se superan estas conexiones, el riesgo de que se produzcan errores de asignación de puertos será mayor. Si se producen errores de asignación de puertos, añada más destinos al grupo de destino.

Al lanzar un equilibrador de carga de red en una VPC compartida (como participante), solo puede registrar destinos en las subredes que se hayan compartido con usted.

Cuando el tipo de destino es `alb`, puede registrar un único equilibrador de carga de aplicación como destino. Para obtener más información, consulte Utilice un equilibrador de carga de aplicaciones como destino de un equilibrador de carga de red.

Los equilibradores de carga de red no admiten el tipo de destino `lambda`. Los equilibradores de carga de aplicación son los únicos equilibradores de carga que admiten el tipo de destino `lambda`. Para obtener más información, consulte Funciones de Lambda como destinos en la Guía del usuario de Equilibradores de carga de aplicación.

Si tiene microservicios en instancias registradas con un equilibrador de carga de red, no puede usar el equilibrador de carga para establecer una comunicación entre ellos, a menos que el equilibrador de carga esté expuesto a Internet o las instancias estén registradas mediante una dirección IP. Para obtener más información, consulte Se agota el tiempo de espera de conexión para las solicitudes enviadas desde un destino a su balanceador de carga.

Solicitud de direcciones IP y de enrutamiento

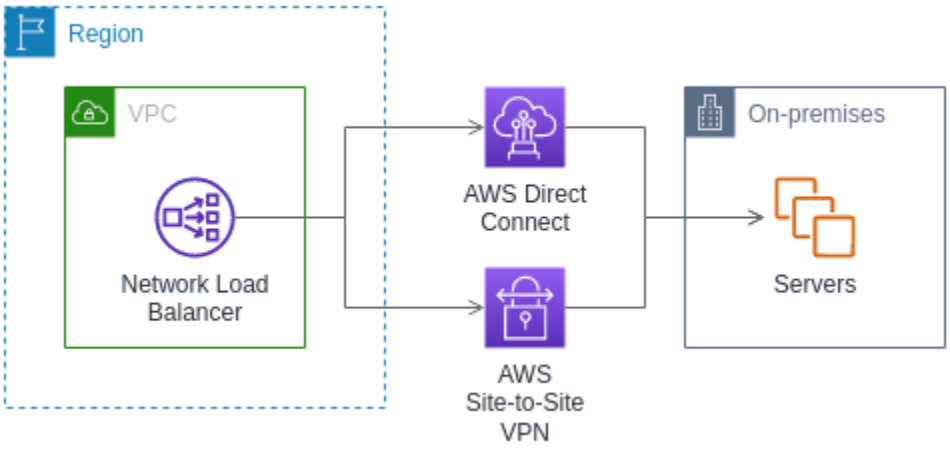
Si especifica destinos utilizando un ID de instancia, el tráfico se redirige a las instancias utilizando la dirección IP privada principal especificada en la interfaz de red principal de la instancia. El balanceador de carga vuelve a escribir la dirección IP de destino del paquete de datos antes de reenviarla a la instancia de destino.

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. Tenga en cuenta que cada interfaz de red puede tener su propio grupo de seguridad. El balanceador de carga vuelve a escribir la dirección IP de destino antes de reenviarla al destino.

Para obtener más información acerca de cómo permitir el tráfico a las instancias, consulte Grupos de seguridad de destino.

Recursos en las instalaciones como destinos

Los recursos locales vinculados mediante una conexión de VPN Site-to-Site o Direct Connect pueden servir de destino, cuando el tipo de destino es `ip`.



Cuando se utilizan recursos en las instalaciones, las direcciones IP de estos destinos deben provenir de uno de los siguientes bloques de CIDR:

- 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)

Para obtener más información acerca del Direct Connect, consulte ¿Qué es el Direct Connect?

Para obtener más información acerca del AWS Site-to-Site VPN, consulte ¿Qué es el AWS Site-to-Site VPN?

Tipo de dirección IP

Al crear un nuevo grupo de destino, puede seleccionar el tipo de dirección IP de su grupo de destino. Esto controla la versión de IP utilizada para comunicarse con los destinos y comprobar su estado.

Los grupos de destino de los equilibradores de carga de red admiten los siguientes tipos de direcciones IP:

`ipv4`

El equilibrador de carga se comunica con los destinos mediante IPv4.

`ipv6`

El equilibrador de carga se comunica con los destinos mediante IPv6.

Consideraciones

- El equilibrador de carga se comunica con los destinos en función del tipo de dirección IP del grupo de destino. Los destinos de un grupo de destinos IPv4 deben aceptar tráfico IPv4 procedente del equilibrador de carga, y los destinos de un grupo de destinos IPv6 deben aceptar tráfico IPv6 procedente del equilibrador de carga.
- No puede utilizar un grupo de destinos IPv6 con un equilibrador de carga `ipv4`.
- No puede usar un grupo de destino IPv4 con un oyente UDP para un equilibrador de carga `dualstack`.
- No puede registrar un equilibrador de carga de aplicaciones en un grupo de destino IPv6.
- No puede utilizar un grupo de destino IPv6 con los protocolos QUIC o TCP_QUIC.

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. Cada grupo de destino debe tener al menos

un destino registrado en cada zona de disponibilidad que esté habilitado para el equilibrador de carga. Puede registrar cada destino en uno o varios grupos de destino.

Si aumenta la demanda en la aplicación, puede registrar más destinos en uno o varios grupos para controlar la demanda. El equilibrador de carga comienza a enrutar el tráfico a un destino recién registrado tan pronto como se completa el proceso de registro y el destino supera la primera comprobación de estado inicial, independientemente del umbral configurado.

Si la demanda de la aplicación se reduce o si 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 balanceador de carga deja de direccionar el tráfico 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 tráfico.

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.

Requisitos y consideraciones

- No puede registrar instancias por ID de instancia si usa uno de los siguientes tipos de instancia: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1.
- Al registrar los destinos por ID de instancia para un grupo de destinos de IPv6, los destinos deben tener una dirección IPv6 principal asignada. Para obtener más información, consulte Direcciones IPv6 en la Guía del usuario de Amazon EC2
- Al registrar destinos por ID de instancia, las instancias deben estar en la misma VPC que el equilibrador de carga de red. No puede registrar instancias por ID de instancia si están en una VPC interconectada a la VPC del equilibrador de carga (misma región o región diferente). Puede registrar estas instancias por dirección IP.
- Si registra un destino por dirección IP y la dirección IP está en la misma VPC que el balanceador de carga, el balanceador de carga verifica que proviene de una subred a la que tiene acceso.
- El equilibrador de carga dirige el tráfico a los destinos solo en las zonas de disponibilidad que están habilitadas. Los destinos de las zonas que no están habilitadas no se utilizan.

- En el caso de los grupos de destino UDP, TCP_UDP, QUIC y TCP_QUIC, no registre instancias por dirección IP si residen fuera de la VPC del equilibrador de carga o si utilizan alguno de los siguientes tipos de instancia: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1. Es posible que los destinos que residen fuera de la VPC del equilibrador de carga o que usen un tipo de instancia no compatible puedan recibir tráfico del equilibrador de carga, pero luego no puedan responder.

Atributos del grupo de destino

Puede configurar un grupo de destino editando sus atributos. Para obtener más información, consulte Edición de atributos del grupo de destino.

Los siguientes atributos del grupo de destino son compatibles. Puede modificar estos atributos solo si el tipo de grupo de destino es `instance` o `ip`. Si el tipo de grupo de destino es `alb`, estos atributos siempre utilizan sus valores predeterminados.

`deregistration_delay.timeout_seconds`

Cantidad de tiempo que Elastic Load Balancing espera antes de cambiar el estado de un proceso de anulación del registro de `draining` a `unused`. El rango va de 0 a 3600 segundos. El valor de predeterminado es de 300 segundos. Para el tráfico QUIC, el valor es siempre de 300 segundos.

`deregistration_delay.connection_termination.enabled`

Indica si el equilibrador de carga finaliza las conexiones al final del tiempo de espera de anulación del registro. El valor es `true` o `false`. Para los nuevos grupos de destino de UDP/TCP_UDP, el valor predeterminado es `true`. De lo contrario, el valor predeterminado es `false`. Este atributo no se aplica al tráfico QUIC.

`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`.

`preserve_client_ip.enabled`

Indica si la preservación de IP del cliente está habilitada. El valor es `true` o `false`. El valor predeterminado está deshabilitado si el tipo de grupo de destino es dirección IP y el protocolo de grupo de destino es TCP o TLS. De lo contrario, el valor predeterminado está habilitado.

La conservación de la IP del cliente no se puede desactivar para los grupos de destino UDP, TCP_UDP, QUIC y TCP_QUIC.

`proxy_protocol_v2.enabled`

Indica si Proxy Protocol versión 2 está habilitado. De forma predeterminada, Proxy Protocol está deshabilitado.

`stickiness.enabled`

Indica si están habilitadas las sesiones rápidas. El valor es `true` o `false`. El valor predeterminado es `false`. Este atributo no se aplica al tráfico QUIC.

`stickiness.type`

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

`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 está `off`, la retirada por error de DNS no está habilitada, lo que significa que, incluso si todos los destinos del grupo de destino están en mal estado, la zona no se elimina del DNS. El valor predeterminado 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 valores posibles son `off` o un número entero comprendido entre 1 y 100. Cuando está `off`, la retirada por error de DNS no está habilitada, lo que significa que, incluso si todos los destinos del grupo de destino están en mal estado, la zona no se elimina del DNS. El valor predeterminado es `off`.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

La cantidad mínima de destinos que deben estar en buen estado. Si la cantidad de destinos en buen estado es inferior a este valor, envíe el tráfico a todos los destinos, incluidos los destinos en mal estado. Los valores posibles van del 1 a la cantidad máxima de destinos. El valor predeterminado 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`.

`target_health_state.unhealthy.connection_termination.enabled`

Indica si el equilibrador de carga finaliza las conexiones a destinos en mal estado. El valor es `true` o `false`. El valor predeterminado es `true`.

`target_health_state.unhealthy.draining_interval_seconds`

Cantidad de tiempo que Elastic Load Balancing espera antes de cambiar el estado de un destino en mal estado de `unhealthy.draining` a `unhealthy`. El rango es 0-360 000 segundos. El valor predeterminado es 0 segundos.

Nota: Este atributo solo se puede configurar cuando el valor de `target_health_state.unhealthy.connection_termination.enabled` es `false`.

Estado del grupo de destino

De forma predeterminada, un grupo de destino se considera en buen estado siempre que tenga al menos un destino en buen estado. Si tiene una flota grande, no basta con tener un solo destino en buen estado que atienda el tráfico. En su lugar, puede especificar un recuento o porcentaje mínimo de destinos que deben estar en buen estado y qué acciones tomará el equilibrador de carga cuando los destinos en buen estado estén por debajo del umbral especificado. Esto mejora la disponibilidad de la aplicación.

Contenido

Acciones en mal estado

Puede configurar umbrales de buen estado para las siguientes acciones:

- Conmutación por error de DNS: cuando el número de destinos en buen estado en una zona cae por debajo del umbral, se marcan como en mal estado en DNS las direcciones IP del nodo del equilibrador de carga correspondientes a esa zona. 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 el número de destinos en buen estado en una zona cae por debajo del umbral, el equilibrador de carga envía tráfico a todos los destinos 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

- Si especifica ambos tipos de umbrales para una acción (recuento y porcentaje), el equilibrador de carga realizará la acción cuando se supere alguno de los umbrales.
- Si especifica umbrales para ambas acciones, el umbral de la conmutación por error de DNS debe ser mayor o igual que el umbral de la conmutación por error de enrutamiento, de modo que la conmutación por error de DNS se produzca al mismo tiempo que la conmutación por error de enrutamiento o antes.
- Si especifica el umbral como un porcentaje, calculamos el valor de forma dinámica en función de la cantidad total de destinos registrados en los grupos de destino.
- La cantidad total de destinos se basa en si el equilibrio de carga entre zonas está activado o desactivado. Si el equilibrio de carga entre zonas está desactivado, cada nodo envía tráfico solo a los destinos de su propia zona, lo que significa que los umbrales se aplican a la cantidad de destinos de cada zona habilitada por separado. Si el equilibrio de carga entre zonas está activado, cada nodo envía tráfico a todos los destinos de todas las zonas habilitadas, lo que significa que los umbrales especificados se aplican a la cantidad total de destinos de todas las zonas habilitadas. Para obtener más información, consulte Balance de carga entre zonas.
- Cuando se produce una conmutación por error de DNS, esta afecta a todos los grupos de destinos asociados con el 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, se eliminan del nombre de host de DNS del equilibrador de carga las direcciones IP de las zonas en mal estado. Sin embargo, la memoria caché de DNS del

cliente local puede contener estas direcciones IP hasta que caduque el tiempo de vida (TTL) del registro DNS (60 segundos).

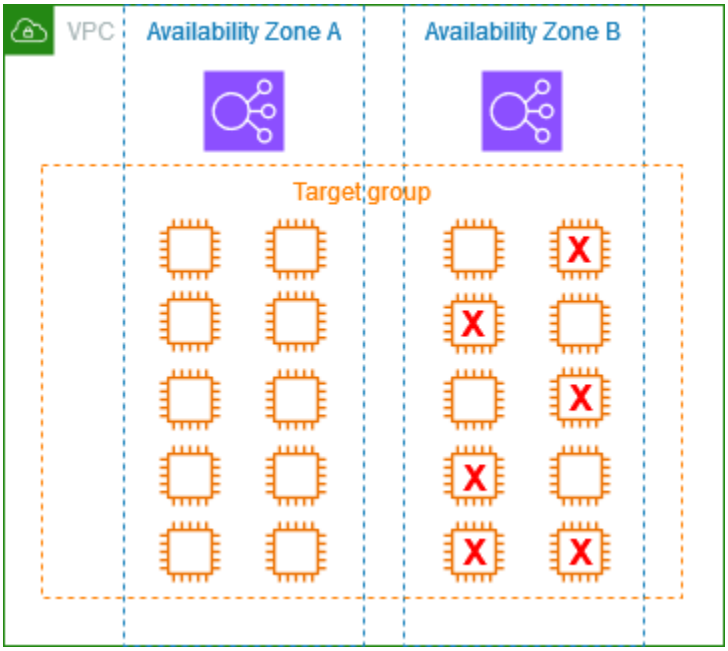
- Con la conmutación por error de DNS, si hay varios grupos de destino asociados a un equilibrador de carga de red y uno de los grupos de destino está en mal estado en una zona, se produce la conmutación por error de DNS, incluso si otro grupo de destino está en buen estado en esa misma zona.
- Con la conmutación por error de DNS, si se considera que todas las zonas del equilibrador de carga están en mal estado, el equilibrador de carga envía tráfico a todas las zonas, incluidas las zonas en mal estado.
- Existen otros factores, además de la existencia de suficientes destinos en buen estado, que podrían provocar una conmutación por error de DNS, como el estado de la zona.

Ejemplo

En el siguiente ejemplo, se muestra cómo se aplica la configuración de estado del grupo de destino.

Escenario

- Un equilibrador de carga que admite dos zonas de disponibilidad, A y B
- Cada zona de disponibilidad contiene 10 destinos registrados
- El grupo de destino tiene la siguiente configuración de estado del grupo de destino:
  - Conmutación por error de DNS: 50 %
  - Conmutación por error de enrutamiento: 50 %
- Seis destinos fallan en la zona de disponibilidad B



Cuando el equilibrio de carga entre zonas está desactivado

- El nodo del equilibrador de carga de cada zona de disponibilidad solo puede enviar tráfico a los 10 destinos de su zona de disponibilidad.
- Hay 10 destinos en buen estado en la zona de disponibilidad A que cumplen con el porcentaje requerido de destinos en buen estado. El equilibrador de carga sigue distribuyendo el tráfico entre los 10 destinos en buen estado.
- Solo hay 4 destinos en buen estado en la zona de disponibilidad B, es decir, el 40% de los destinos del nodo del equilibrador de carga de la zona de disponibilidad B. Como este porcentaje es inferior al porcentaje de destinos en buen estado requerido, el equilibrador de carga toma las siguientes medidas:
  - Conmutación por error de DNS: la zona de disponibilidad B está marcada como en mal estado en el DNS. Como los clientes no pueden resolver el nombre del equilibrador de carga en el nodo del equilibrador de carga de la zona de disponibilidad B y la zona de disponibilidad A está en buen estado, los clientes envían nuevas conexiones a la zona de disponibilidad A.
  - Conmutación por error de enrutamiento: cuando se envían nuevas conexiones de forma explícita a la zona de disponibilidad B, el equilibrador de carga distribuye el tráfico a todos los destinos de la zona de disponibilidad B, incluidos los destinos en mal estado. Esto evita interrupciones entre los demás destinos en buen estado.

Cuando el equilibrio de carga entre zonas está activado

- Cada nodo del equilibrador de carga puede enviar tráfico a los 20 destinos registrados en ambas zonas de disponibilidad.
- Hay 10 destinos en buen estado en la zona de disponibilidad A y 4 destinos en buen estado en la zona de disponibilidad B, con un total de 14 destinos en buen estado. Esto representa el 70% de los destinos de los nodos del equilibrador de carga en ambas zonas de disponibilidad, lo que cumple con el porcentaje requerido de destinos en buen estado.
- El equilibrador de carga distribuye el tráfico entre los 14 destinos en buen estado en ambas zonas de disponibilidad.

Uso de la conmutación por error de DNS de Route 53 para el equilibrador de carga

Si utiliza Route 53 para dirigir las consultas de DNS al equilibrador de carga, también puede utilizar Route 53 para configurar la conmutación por error de DNS del equilibrador de carga. En una configuración de conmutación por error, Route 53 comprueba el estado de los destinos del grupo de destino para el equilibrador de carga con el fin de determinar si están disponibles. Si no existen destinos en buen estado registrados en el equilibrador de carga o si este no se encuentra en buen estado, Route 53 enruta el tráfico a otro recurso disponible, como un equilibrador de carga en buen estado o un sitio web estático en Amazon S3.

Por ejemplo, supongamos que tenemos una aplicación web para `www.example.com` y deseamos ejecutar instancias redundantes por detrás de dos equilibradores de carga que residen en regiones distintas. Queremos enrutar el tráfico principalmente al equilibrador de carga de una de las regiones y utilizar el equilibrador de carga de la otra región como copia de seguridad en caso de error. Si configura la conmutación por error de DNS, puede especificar los equilibradores de carga principal y secundario (de copia de seguridad). Route 53 enruta el tráfico al equilibrador de carga principal si está disponible, o bien, en caso contrario, al secundario.

Cómo funciona la evaluación del estado de los destinos

- Si evaluar el estado del destino está configurado como `Yes` en un registro de alias de un equilibrador de carga de red, Route 53 evalúa el estado del recurso especificado por el valor `alias target`. Route 53 utiliza las comprobaciones de estado del grupo de destinos.
- Si todos los grupos de destino asociados a un equilibrador de carga de red están en buen estado, Route 53 marca el registro de alias como en buen estado. Si configura un umbral para un grupo de

destinos y este cumple dicho umbral, supera las comprobaciones de estado. De lo contrario, si un grupo de destinos contiene al menos un destino en buen estado, supera las comprobaciones de estado. Si las comprobaciones de estado se superan, Route 53 devuelve los registros de acuerdo con la política de enrutamiento. Si se utiliza una política de enrutamiento de conmutación por error, Route 53 devuelve el registro principal.

- Si todos los grupos de destino asociados a un equilibrador de carga de red están en mal estado, el registro de alias no supera la comprobación de estado de Route 53 (apertura por error). Si se utiliza evaluar el estado del destino, esto provoca que la política de enrutamiento de conmutación por error redirija el tráfico al recurso secundario.
- Si todos los grupos de destino de un equilibrador de carga de red están vacíos (sin destinos), Route 53 considera el registro en mal estado (apertura por error). Si se utiliza evaluar el estado del destino, esto provoca que la política de enrutamiento de conmutación por error redirija el tráfico al recurso secundario.

Para obtener más información, consulte Uso de umbrales de comprobación de estado de grupos de destinos del equilibrador de carga para mejorar la disponibilidad en el Blog de AWS, y Configuración de la conmutación por error de DNS en la Guía para desarrolladores de Amazon Route 53.

Para crear un grupo de destino para el equilibrador de carga de red

Los destinos del equilibrador de carga de red se registran mediante 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.

Para direccionar el tráfico a los destinos de un grupo de destino, cree un agente de escucha y especifique el grupo de destino en la acción predeterminada del agente de escucha. Para obtener más información, consulte Acciones predeterminadas. Puede especificar el mismo grupo de destino en varios oyentes, pero estos oyentes deben pertenecer al mismo equilibrador de carga de red. Para usar un grupo de destino con un equilibrador de carga, debe comprobar que un oyente no esté usando el grupo de destino para otro equilibrador de carga.

Puede agregar o eliminar destinos del grupo de destino en cualquier momento. Para obtener más información, consulte Registro de destinos del equilibrador de carga de red. También puede modificar la configuración de la comprobación de estado del grupo de destino. Para obtener más información, consulte Actualización de la configuración de comprobación de estado del grupo de destino de un equilibrador de carga de red.

Requisitos

- Después de crear un grupo de destino, no puede cambiar su tipo de destino ni su tipo de dirección IP.
- Todos los destinos de un grupo de destino deben tener el mismo tipo de dirección IP que el grupo de destino: IPv4 o IPv6.
- Debe utilizar un grupo de destino IPv6 con un equilibrador de carga de pila doble.
- No puede usar un grupo de destino IPv4 con un oyente UDP para un equilibrador de carga `dualstack`.
- No puede utilizar un grupo de destino IPv6 con los protocolos QUIC o TCP_QUIC.

Console

Creación de un grupo de destino

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 el panel de Configuración básica, haga lo siguiente:

   a. En Elegir un tipo de destino, seleccione Instancias para registrar los destinos por ID de instancia, Direcciones IP a fin de registrar los destinos por dirección IP o Equilibrador de carga de aplicación para registrar un equilibrador de carga de aplicación como destino.

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

   c. En Protocol (Protocolo), elija un protocolo tal y como se indica a continuación:

      - Si el protocolo del agente de escucha es TCP, elija TCP o TCP_UDP.
      - Si el protocolo del agente de escucha es TLS, elija TCP o TLS.
      - Si el protocolo del agente de escucha es UDP, elija UDP o TCP_UDP.
      - Si el protocolo del agente de escucha es TCP_UDP, elija TCP_UDP.
      - Si el protocolo del oyente es QUIC, seleccione QUIC.
      - Si el protocolo del oyente es TCP_QUIC, seleccione TCP_QUIC.

- Si el tipo de destino es Equilibrador de carga de aplicaciones, el protocolo debe ser TCP.

d. En Puerto, modifique el valor predeterminado según sea necesario.

   Si el tipo de destino es Equilibrador de carga de aplicaciones, el puerto debe coincidir con el puerto del oyente del equilibrador de carga de aplicaciones.

e. En Tipo de dirección IP, elija IPv4 o IPv6. Esta opción está disponible solo si el tipo de destino es Instancias o Direcciones IP.

f. En VPC, seleccione la nube privada virtual (VPC) con los destinos que desee registrar.

5. En el panel de Comprobaciones de estado, modifique la configuración predeterminada según sea necesario. 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 ???.
6. (Opcional) Para agregar una etiqueta, expanda Etiquetas, elija Agregar etiqueta e ingrese una clave y un valor de etiqueta.
7. Elija Siguiente.
8. (Opcional) Registre destinos. El tipo de destino del grupo de destino determina la información que debe proporcionar. Si aún no está listo para registrar destinos, puede hacerlo más adelante.
   - Instancias: seleccione las instancias de EC2, introduzca los puertos y elija Incluir como pendientes a continuación.
   - Direcciones IP: seleccione la VPC que contiene las direcciones IP u Otras direcciones IP privadas, introduzca las direcciones IP y los puertos, y seleccione Incluir como pendientes a continuación.
   - Equilibrador de carga de aplicaciones: seleccione el equilibrador de carga de aplicaciones. Para obtener más información, consulte Uso de equilibradores de carga de aplicación como destinos.
9. Elija Crear grupo de destino.

AWS CLI

Creación de un grupo de destino

Utilice el comando create-target-group. El siguiente ejemplo crea un grupo de destino con el protocolo TCP, destinos registrados por dirección IP, una etiqueta y la configuración predeterminada de comprobación de estado.

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type ip \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

Para registrar destinos

Use el comando register-targets para registrar destinos en el grupo de destinos. Para ver ejemplos, consulte the section called “Cómo registrar destinos”.

CloudFormation

Creación de un grupo de destino

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::TargetGroup. El siguiente ejemplo crea un grupo de destinos con el protocolo TCP, destinos registrados por dirección IP, una única etiqueta, la configuración predeterminada de comprobación de estado y dos destinos registrados.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: 10.0.50.10
          Port: 80
        - Id: 10.0.50.20
          Port: 80
```

Actualización de la configuración de estado del grupo de destino del equilibrador de carga de red

De forma predeterminada, los equilibradores de carga de red supervisan el estado de los destinos y enrutan las solicitudes hacia los destinos en buen estado. Sin embargo, si el equilibrador de carga no dispone de suficientes destinos en buen estado, envía automáticamente el tráfico a todos los destinos registrados. Puede modificar la configuración de estado del grupo de destinos para definir los umbrales de conmutación por error de DNS y conmutación por error de enrutamiento. Para obtener más información, consulte the section called “Estado del grupo de destino”.

Console

Para actualizar la configuración de comprobación de estado del grupo de destino

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. Amplíe los requisitos de estado del grupo de destino.
6. En Tipo de configuración, recomendamos que seleccione Configuración unificada, que establece el mismo umbral tanto para la conmutación por error de DNS como para la conmutación por error de enrutamiento.
7. 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.
8. El texto informativo indica si el equilibrio de carga entre zonas está habilitado para el grupo de destino. Si el equilibrio de carga entre zonas está desactivado, puede habilitarlo para asegurarse de que dispone de capacidad suficiente. En Configuración de selección de destino, actualice Equilibrio de carga entre zonas.

   El siguiente texto indica que el equilibrio de carga entre zonas está desactivado:

```
Healthy state requirements apply to each zone independently.
```

El siguiente texto indica que el equilibrio de carga entre zonas está habilitado:

```
Healthy state requirements apply to the total targets across all applicable
 zones.
```

9. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar la configuración de comprobación de estado del grupo de destino

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 target-group-arn \
    --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=5
```

CloudFormation

Para modificar la configuración de estado del grupo de destinos

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup. En el siguiente ejemplo, se establece el umbral de buen estado para ambas acciones de mal estado en un 50 %.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_group_health.dns_failover.minimum_healthy_targets.percentage"
```

```
          Value: "50"
        - Key:
"target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage"
          Value: "50"
```

Comprobaciones de estado de grupos de destino del equilibrador de carga de red

Puede registrar los destinos en uno o varios grupos de destino. El equilibrador de carga comienza a enrutar las solicitudes hacia un destino recién registrado tan pronto como se completa el proceso de registro y los destinos superan las comprobaciones de estado iniciales. El proceso de registro puede tardar unos minutos en completarse y comenzar las comprobaciones de estado.

Los equilibradores de carga de red utilizan comprobaciones de estado activas y pasivas para determinar si un destino se encuentra disponible para administrar solicitudes. De forma predeterminada cada uno de los nodos del balanceador de carga direcciona las solicitudes exclusivamente a los destinos en buen estado de su zona de disponibilidad. Si se habilita el balanceo de carga entre zonas, cada nodo del balanceador de carga direccionará el tráfico entre los destinos en buen estado de todas las zonas de disponibilidad habilitadas. Para obtener más información, consulte Balance de carga entre zonas.

Con las comprobaciones de estado pasivas, el balanceador de carga observa cómo los objetivos responden a las conexiones. Las comprobaciones de estado pasivas permiten que el balanceador de carga pueda detectar un destino en mal estado antes de que lo notifiquen las comprobaciones de estado activas. Las comprobaciones de estado pasivas no se pueden deshabilitar, configurar ni monitorear. Las comprobaciones de estado pasivas no son compatibles con el tráfico UDP, ni con grupos de destino con la persistencia activada. Para obtener más información, consulte Sesiones persistentes.

Si un destino no se encuentra en buen estado, el equilibrador de carga envía un RST de TCP para los paquetes recibidos en las conexiones de cliente asociadas al destino, a menos que el destino en mal estado active el modo de apertura por error en el equilibrador de carga.

Si los grupos de destino no tienen un destino en buen estado en una zona de disponibilidad habilitada, se quita del DNS la dirección IP de la subred correspondiente, para que no puedan dirigirse solicitudes a esa zona de disponibilidad. Si todos los destinos no pasan las comprobaciones de estado a la vez en todas las zonas de disponibilidad habilitadas, se produce un error al abrir el equilibrador de carga. Los equilibradores de carga de red quedarán en estado de apertura por error

si tiene un grupo de destino vacío. 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.

Si un grupo de destino se encuentra configurado con comprobaciones de estado de HTTPS, sus destinos registrados no pasarán las comprobaciones de estado si solo admiten TLS 1.3. Estos destinos deben ser compatibles con una versión anterior de TLS, como TLS 1.2.

En las solicitudes de comprobación de estado HTTP o HTTPS, el encabezado de host contiene la dirección IP del nodo del balanceador de carga y el puerto del agente de escucha, no la dirección IP del destino y el puerto de comprobación de estado.

Si agrega un oyente de TLS a su equilibrador de carga de red, realizaremos una prueba de conectividad del oyente. Como la terminación de TLS también termina una conexión TCP, se establece una nueva conexión TCP entre el balanceador de carga y los destinos. Por tanto, es posible que observe que se envían las conexiones TCP de esta prueba desde el equilibrador de carga a los destinos que estén registrados en el oyente TLS. Puede identificar estas conexiones TCP, ya que tienen la dirección IP de origen del equilibrador de carga de red y las conexiones no contienen paquetes de datos.

En el caso de los servicios UDP y QUIC, la disponibilidad del destino se puede revisar mediante comprobaciones de estado que no sean UDP en el grupo de destino. Puede utilizar cualquier comprobación de estado disponible (TCP, HTTP o HTTPS) y cualquier puerto en el destino para verificar la disponibilidad del servicio. Si se produce un error del servicio que recibe la comprobación de estado, se considera que el destino no se encuentra disponible. Para mejorar la precisión de las comprobaciones de estado del servicio, configure el servicio para que escuche en el puerto de comprobación de estado, con el fin de realizar el seguimiento del estado del servicio UDP o QUIC y marcar como fallida la comprobación de estado si el servicio no está disponible.

Para obtener más información, consulte the section called “Estado del grupo de destino”.

Contenido

Configuración de comprobación de estado

Puede utilizar los siguientes ajustes para configurar las comprobaciones de estado activas en los destinos de un grupo de destino. Si las comprobaciones de estado superan el umbral de UnhealthyThresholdCount errores consecutivos, el equilibrador de carga inhabilita el destino. Cuando las comprobaciones de estado superan el umbral de HealthyThresholdCount éxitos consecutivos, el equilibrador de carga vuelve a poner el destino en servicio.

Ajuste	Descripción	Predeterminado
HealthCheckProtocol	Protocolo que el equilibrador de carga utiliza al realizar comprobaciones de estado en los destinos. Los posibles protocolos son HTTP, HTTPS y TCP. El valor predeterminado es el protocolo TCP. Si el tipo de destino es `alb`, los protocolos de comprobación de estado admitidos son HTTP y HTTPS.	TCP
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.	El puerto en el que cada destino recibe el tráfico procedente del equilibrador de carga.
HealthCheckPath	[Comprobaciones de estado HTTP/HTTPS] Ruta de comprobación de estado asignada a los destinos para las comprobaciones de estado. El valor predeterminado es /.	/
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. Los valores	6 segundos para las comprobaciones de

Ajuste	Descripción	Predeterminado
	predeterminados son de 6 segundos para las comprobaciones de estado de HTTP y de 10 segundos para las comprobaciones de estado de TCP y HTTPS.	estado de HTTP y 10 segundos para las comprobaciones de estado de TCP y HTTPS.
HealthCheckIntervalSeconds	Cantidad aproximada de tiempo, en segundos, que transcurre entre comprobaciones de estado de un destino individual. El rango va de 5 a 300 segundos. El valor predeterminado es de 30 segundos. Las comprobaciones de estado de un equilibrador de carga de red se distribuyen y utilizan un mecanismo de consenso para determinar el estado del destino. Por tanto, los destinos reciben un número mayor de comprobaciones de estado que el que está establecido. Para reducir el impacto en los destinos si utiliza comprobaciones de estado de HTTP, use un objetivo más sencillo en los destinos, como, por ejemplo, un archivo HTML estático, o cambie a las comprobaciones de estado de TCP.	30 segundos
HealthyThresholdCount	Número de comprobaciones de estado consecutivas que deben superarse para considerar que un destino en mal estado vuelve a estar en buen estado. El rango va de 2 a 10. El valor predeterminado es 5.	5

Ajuste	Descripción	Predeterminado
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.	2
Matcher	[Comprobaciones de estado HTTP/HTTPS] Códigos HTTP que se deben utilizar al comprobar si se ha recibido una respuesta correcta de un destino. El rango va de 200 a 599. El valor predeterminado va de 200 a 399.	200-399

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.

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. Códigos de motivo relacionados: `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	El destino se encuentra en buen estado. Códigos de motivo relacionados: ninguno

Valor	Descripción
`unhealthy`	El destino no ha respondido a una comprobación de estado, no la ha superado o se encuentra en estado de detención. Código de motivo relacionado: `Target.FailedHealthChecks`
`draining`	El destino está en proceso de anulación del registro y de vaciado de conexiones. Código de motivo relacionado: `Target.DeregistrationInProgress`
`unhealthy.draining`	El destino no ha respondido a una comprobación de estado, o no la ha superado y entra en periodo de gracia. El destino admite las conexiones existentes y no aceptará ninguna conexión nueva durante este periodo de gracia. Código de motivo relacionado: `Target.FailedHealthChecks`
`unavailable`	El estado del destino no está disponible. Código de motivo relacionado: `Elb.InternalError`
`unused`	El destino no está registrado en un grupo de destino, el grupo de destino no se utiliza en una regla de oyente o el destino se encuentra en una zona de disponibilidad que no está habilitada. Códigos de motivo relacionados: `Target.NotRegistered` | `Target.NotInUse` | `Target.InvalidState` | `Target.IpUnusable`

Códigos de motivo de comprobación de estado

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

Código de motivo	Descripción
`Elb.InitialHealthChecking`	Las comprobaciones de estado iniciales están en curso.
`Elb.InternalError`	Las comprobaciones de estado no se han superado debido a un error interno.
`Elb.RegistrationInProgress`	El registro del destino está en curso.
`Target.DeregistrationInProgress`	La anulación del registro del destino está en curso.
`Target.FailedHealthChecks`	Las comprobaciones de estado no se han superado.
`Target.InvalidState`	El destino se encuentra en estado detenido. El destino se encuentra en estado terminado. El destino se encuentra en estado terminado o detenido. El destino se encuentra en un estado no válido.
`Target.IpUnusable`	La dirección IP no se puede utilizar como destino, ya que la utiliza un equilibrador de carga.
`Target.NotInUse`	El grupo de destino no se ha configurado para recibir el tráfico del equilibrador de carga. El destino se encuentra en una zona de disponibilidad que no está habilitada para el equilibrador de carga.

Código de motivo	Descripción
`Target.NotRegistered`	El destino no está registrado en el grupo de destino.

Comprobación del estado de los destinos del equilibrador de carga de red

Puede comprobar el estado de los destinos registrados en los grupos de destino. Para obtener ayuda con errores en la comprobación de estado, consulte Solución de problemas: un destino registrado no está en servicio.

Console

Para comprobar el estado de los destinos

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 el pestaña Detalles se muestra la cantidad total de destinos, más la cantidad de destinos de cada estado.
5. En la pestaña de Destinos, la columna de Estado indica el estado de cada destino.
6. Si el estado de un destino es un valor distinto de `Healthy`, la columna de Detalles del estado contiene más información.

Para recibir notificaciones por correo electrónico sobre destinos en mal estado

Utilice alarmas de CloudWatch para activar una función de Lambda y enviar detalles sobre los destinos en mal estado. Para obtener instrucciones paso a paso, consulte la siguiente entrada de blog: Identificar destinos en mal estado del equilibrador de carga.

AWS CLI

Para comprobar el estado de los destinos

Utilice el comando describe-target-health. Este ejemplo filtra la salida para incluir solo los destinos que no están en buen estado. En el caso de los destinos que no están en buen estado, la salida incluye un código de motivo.

```
aws elbv2 describe-target-health \
```

```
    --target-group-arn target-group-arn \
    --query "TargetHealthDescriptions[?TargetHealth.State!='healthy'].
[Target.Id,TargetHealth.State,TargetHealth.Reason]" \
    --output table
```

A continuación, se muestra un ejemplo del resultado.

```
-----------------------------------------------
|            DescribeTargetHealth             |
+--------------+---------+--------------------+
|  172.31.0.57 |  unused |  Target.NotInUse   |
|  172.31.0.50 |  unused |  Target.NotInUse   |
+--------------+---------+--------------------+
```

Estados de los destinos y códigos de motivo

La siguiente lista muestra los posibles códigos de motivo para cada estado de destino.

El estado del destino es healthy

No se proporciona un código de motivo.

El estado del destino es initial

- `Elb.RegistrationInProgress`: el destino está en proceso de registro en el equilibrador de carga.
- `Elb.InitialHealthChecking`: el equilibrador de carga todavía envía al destino la cantidad mínima de comprobaciones de estado necesarias para determinar su estado.

El estado del destino es unhealthy

- `Target.FailedHealthChecks`: el equilibrador de carga recibió un error al intentar establecer una conexión con el destino o la respuesta del destino tenía un formato que no es válido.

El estado del destino es unused

- `Target.NotRegistered`: el destino no está registrado en el grupo de destinos.
- `Target.NotInUse`: el grupo de destinos no es utilizado por ningún equilibrador de carga, o el destino se encuentra en una zona de disponibilidad que no está habilitada para su equilibrador de carga.
- `Target.InvalidState`: el destino se encuentra en estado detenido o terminado.

- `Target.IpUnusable`: la dirección IP del destino está reservada para uso de un equilibrador de carga.

El estado del destino es draining

- `Target.DeregistrationInProgress`: el destino está en proceso de anulación de registro y el periodo de retardo para la anulación aún no ha caducado.

El estado del destino es unavailable

- `Elb.InternalError`: el estado del destino no está disponible debido a un error interno.

Actualización de la configuración de comprobación de estado del grupo de destino de un equilibrador de carga de red

Puede actualizar la configuración de comprobación de estado del grupo de destino en cualquier momento. Para ver la lista de configuraciones de comprobación de estado, consulte the section called “Configuración de comprobación de estado”.

Console

Para actualizar las configuraciones de comprobación de estado

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 abrir la página de detalles.
4. En la pestaña Health check, elija Edit.
5. En la página Editar configuraciones de comprobación de estado, modifique los parámetros según sea necesario.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para actualizar las configuraciones de comprobación de estado

Utilice el comando modify-target-group. El siguiente ejemplo actualiza las configuraciones HealthyThresholdCount y HealthCheckTimeoutSeconds.

```
aws elbv2 modify-target-group \
```

```
    --target-group-arn target-group-arn \
    --healthy-threshold-count 3 \
    --health-check-timeout-seconds 20
```

CloudFormation

Para actualizar las configuraciones de comprobación de estado

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir las configuraciones de comprobación de estado actualizadas. El siguiente ejemplo actualiza las configuraciones HealthyThresholdCount y HealthCheckTimeoutSeconds.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      HealthyThresholdCount: 3
      HealthCheckTimeoutSeconds: 20
```

Edición de atributos del grupo de destino del equilibrador de carga de red

Después de crear un grupo de destino para el equilibrador de carga de red, puede editar los atributos del grupo de destino.

Atributos del grupo de destino

- Preservación de la IP del cliente
- Retardo de anulación del registro
- Protocolo de proxy
- Sesiones rápidas
- Equilibrio de carga entre zonas para grupos de destino
- Interrupción de la conexión para destinos en mal estado

- Intervalo de drenaje para destinos en mal estado

Preservación de la IP del cliente

Los equilibradores de carga de red pueden conservar las direcciones IP de origen de los clientes al enrutar solicitudes hacia los destinos de backend. Cuando se deshabilita la conservación de la IP del cliente, la dirección IP de origen es la dirección IP privada del equilibrador de carga de red.

De forma predeterminada, la conservación de la IP del cliente está habilitada (y no se puede desactivar) para los grupos de destino de tipo instancia y de tipo IP que utilicen los protocolos UDP, TCP_UDP, QUIC y TCP_QUIC. Sin embargo, puede habilitar o deshabilitar la preservación de la IP del cliente para los grupos de destino de TCP y TLS mediante el atributo de grupo de destino `preserve_client_ip.enabled`.

Configuración predeterminada

- Grupos de destino de tipo de instancia: habilitados
- Grupos de destino de tipo IP (UDP, TCP_UDP, QUIC, TCP_QUIC): habilitado
- Grupos de destino de tipo de IP (TCP, TLS): deshabilitados

Cuando la conservación de la IP del cliente está habilitada

La siguiente tabla describe las direcciones IP que reciben los destinos cuando la conservación de la IP del cliente está habilitada.

Targets	Solicitudes de cliente IPv4	Solicitudes de cliente IPv6
Tipo de instancia (IPv4)	Dirección IPv4 del cliente	Dirección IPv4 del equilibrador de carga
Tipo IP (IPv4)	Dirección IPv4 del cliente	Dirección IPv4 del equilibrador de carga
Tipo IP (IPv6)	Dirección IPv6 del equilibrador de carga	Dirección IPv6 del cliente

Cuando la conservación de la IP del cliente está desactivada

La siguiente tabla describe las direcciones IP que reciben los destinos cuando la conservación de la IP del cliente está desactivada.

Targets	Solicitudes de cliente IPv4	Solicitudes de cliente IPv6
Tipo de instancia (IPv4)	Dirección IPv4 del equilibrador de carga	Dirección IPv4 del equilibrador de carga
Tipo IP (IPv4)	Dirección IPv4 del equilibrador de carga	Dirección IPv4 del equilibrador de carga
Tipo IP (IPv6)	Dirección IPv6 del equilibrador de carga	Dirección IPv6 del equilibrador de carga

Requisitos y consideraciones

- Los cambios en la preservación de la IP del cliente solo se aplican a las nuevas conexiones TCP.
- Cuando la conservación de la IP del cliente está habilitada, el tráfico debe fluir directamente del equilibrador de carga de red al destino. El destino debe estar ubicado en la misma VPC que el equilibrador de carga o en una VPC emparejada en la misma región.
- La conservación de la IP del cliente no es compatible cuando se accede a los destinos a través de una puerta de enlace de tránsito.
- La conservación de la IP del cliente no es compatible cuando se utiliza un punto de conexión de equilibrador de carga de puerta de enlace para inspeccionar el tráfico entre el equilibrador de carga de red y el destino (instancia o dirección IP), incluso si el destino se encuentra en la misma VPC que el equilibrador de carga de red.
- Los siguientes tipos de instancia no admiten la preservación de IP del cliente: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 y T1. Se recomienda registrar estos tipos de instancias como direcciones IP con la preservación de la IP del cliente deshabilitada.
- La preservación de la IP del cliente no afecta al tráfico entrante procedente de AWS PrivateLink. La dirección IP de origen del tráfico AWS PrivateLink es siempre la dirección IP privada del equilibrador de carga de red.
- La conservación de la IP del cliente no es compatible cuando un grupo de destino contiene interfaces de red de AWS PrivateLink o la interfaz de red de otro equilibrador de carga de red. Esto provoca una pérdida de comunicación con esos destinos.

- La preservación de la IP del cliente no afecta al tráfico que se modificó de IPv6 a IPv4. La dirección IP de origen de este tipo de tráfico es siempre la dirección IP privada del equilibrador de carga de red.
- Al especificar los destinos por tipo de equilibrador de carga de aplicación, el equilibrador de carga de red conserva la IP del cliente de todo el tráfico entrante y la envía al equilibrador de carga de aplicación. Luego, el equilibrador de carga de aplicación agrega la IP del cliente al encabezado de la solicitud `X-Forwarded-For` antes de enviarla al destino.
- El bucle invertido de NAT, también conocido como horquilla, no se admite cuando la preservación de la IP del cliente está habilitada. Esto ocurre cuando se utilizan equilibradores de carga de red internos y el destino registrado detrás de un equilibrador de carga de red crea conexiones con ese mismo equilibrador de carga de red. La conexión se puede enrutar hacia el destino que intenta crear la conexión, lo que provoca errores de conexión. Recomendamos no conectarse a un equilibrador de carga de red desde destinos que se encuentren detrás de ese mismo equilibrador de carga; como alternativa, también puede evitar este tipo de errores de conexión si desactiva la conservación de la IP del cliente. Si necesita la dirección IP del cliente, puede recuperarla mediante Proxy Protocol v2. Para obtener más información, consulte Protocolo de proxy.
- Cuando la preservación de la IP del cliente está deshabilitada, un equilibrador de carga de red admite 55 000 conexiones simultáneas o alrededor de 55 000 conexiones por minuto a cada destino único (dirección IP y el puerto). Si se superan estas conexiones, el riesgo de que se produzcan errores de asignación de puertos será mayor, y esto provocará fallas al establecer nuevas conexiones. Para obtener más información, consulte Errores de asignación de puertos para flujos de backend.

Console

Para modificar la conservación de la IP del cliente

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 Atributos, seleccione Editar y localice el panel Configuración de tráfico.
5. Para habilitar la preservación de la IP del cliente, active Conservar las direcciones IP de los clientes. Para deshabilitar la preservación de la IP del cliente, desactive Conservar las direcciones IP de los clientes.

6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar la conservación de la IP del cliente

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

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=preserve_client_ip.enabled,Value=true"
```

CloudFormation

Para habilitar la conservación de la IP del cliente

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir el atributo `preserve_client_ip.enabled`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "preserve_client_ip.enabled"
          Value: "true"
```

Retardo de anulación del registro

Cuando se anula el registro de un destino, el equilibrador de carga deja de crear nuevas conexiones con el destino. El balanceador de carga utiliza el vaciado de conexiones para garantizar que el tráfico en tránsito se completa en las conexiones existentes. Si el destino cuyo registro se ha anulado se mantiene en buen estado y no hay ninguna conexión existente inactiva, el equilibrador de carga

puede continuar enviando tráfico al destino. Para garantizar el cierre de las conexiones existentes, puede hacer algo de lo siguiente: habilitar el atributo del grupo de destino para finalizar la conexión, comprobar si la instancia está en mal estado antes de cancelar su registro o cerrar periódicamente las conexiones de los clientes.

El estado inicial de un destino cuyo registro se ha anulado es `draining`, y mientras se encuentre en este estado el destino dejará de recibir nuevas conexiones. No obstante, es posible que el destino siga recibiendo conexiones debido al retraso en la propagación de la configuración. De forma predeterminada, el balanceador de carga cambia el estado de un destino de anulación del registro a `unused` después de 300 segundos. Para cambiar el tiempo que el balanceador de carga espera antes de cambiar el estado de un destino de anulación de registro a `unused`, actualice el valor del retardo de anulación de registro. Recomendamos que especifique un valor de al menos 120 segundos para asegurarse de que se completan las solicitudes. Para el tráfico QUIC, el valor es siempre de 300 segundos y no se puede ajustar.

Si habilita el atributo de grupo de destino para la finalización de la conexión, las conexiones a los destinos cuyo registro se ha anulado se cerrarán poco después de que finalice el tiempo de espera para anular el registro.

Console

Para modificar los atributos de retardo de anulación de registro

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 abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Para cambiar el tiempo de espera de la anulación del registro, introduzca un nuevo valor para Retardo de anulación del registro. Para asegurarse de que las conexiones existentes se cierren después de anular el registro de los destinos, seleccione Terminar conexiones al anular el registro.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para modificar los atributos de retardo de anulación de registro

Utilice el comando modify-target-group-attributes con los atributos `deregistration_delay.timeout_seconds` y `deregistration_delay.connection_termination.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \
      "Key=deregistration_delay.timeout_seconds,Value=60" \
      "Key=deregistration_delay.connection_termination.enabled,Value=true"
```

CloudFormation

Para modificar los atributos de retardo de anulación de registro

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir los atributos `deregistration_delay.timeout_seconds` y `deregistration_delay.connection_termination.enabled`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "deregistration_delay.timeout_seconds"
          Value: "60"
        - Key: "deregistration_delay.connection_termination.enabled"
          Value: "true"
```

Protocolo de proxy

Los equilibradores de carga de red usan la versión 2 de Proxy Protocol para enviar información adicional sobre la conexión, como el origen y el destino. La versión 2 del protocolo de proxy proporciona una codificación binaria del encabezado del protocolo de proxy.

Con oyentes de TCP, el equilibrador de carga antepone un encabezado de protocolo de proxy a los datos de TCP. No descarta ni sobrescribe los datos existentes, incluidos los encabezados

de protocolo de proxy entrante enviados por el cliente u otros proxy, equilibradores de carga o servidores de la ruta de red. Por tanto, es posible recibir más de un encabezado de protocolo proxy. Además, si existe otra ruta de red hacia los destinos fuera del equilibrador de carga de red, es posible que el primer encabezado de protocolo de proxy no corresponda al equilibrador de carga.

Los oyentes de TLS no admiten conexiones entrantes con encabezados de protocolo de proxy enviados por el cliente o cualquier otro servidor proxy.

El tráfico QUIC no admite el protocolo proxy, versión 2.

Si especifica los destinos por dirección IP, las direcciones IP de origen que se proporcionan a las aplicaciones dependen del protocolo del grupo de destino, de la siguiente manera:

- TCP y TLS: De manera predeterminada, la conservación de la IP del cliente está deshabilitada y las direcciones IP de origen proporcionadas a las aplicaciones son las direcciones IP privadas de los nodos del equilibrador de carga. Para conservar la dirección IP del cliente, asegúrese de que el destino se encuentre en la misma VPC, o en una VPC interconectada, y habilite la conservación de la IP del cliente. Si necesita la dirección IP del cliente y no se cumplen estas condiciones, habilite Proxy Protocol y obtenga la dirección IP del cliente del encabezado de Proxy Protocol.
- UDP y TCP_UDP: Las direcciones IP de origen son las direcciones IP de los clientes, ya que la conservación de la IP del cliente está habilitada de manera predeterminada para estos protocolos y no se puede deshabilitar. Si especifica los destinos por ID de instancia, las direcciones IP de origen que se proporcionan a sus aplicaciones son las direcciones IP de los clientes. Sin embargo, si lo prefiere, puede habilitar el protocolo de proxy y obtener las direcciones IP de los clientes del encabezado del protocolo de proxy.

Conexiones de comprobación de estado

Después de habilitar el protocolo de proxy, el encabezado del protocolo de proxy también se incluye en las conexiones de comprobación de estado del equilibrador de carga. Sin embargo, con estas, la información de conexión del cliente no se envía en el encabezado Proxy Protocol.

Los destinos pueden no superar las comprobaciones de estado si no pueden analizar el encabezado del protocolo proxy. Por ejemplo, pueden devolver el siguiente error: HTTP 400: Solicitud incorrecta.

Servicios de punto de conexión de VPC

Para el tráfico procedente de los consumidores del servicio a través de un servicio de punto de conexión de la VPC, las direcciones IP de origen que se proporcionan a sus aplicaciones son las

direcciones IP privadas de los nodos del balanceador de carga. Si sus aplicaciones requieren las direcciones IP de los consumidores del servicio, habilite el protocolo de proxy y obténgalas del encabezado del protocolo de proxy.

El encabezado Proxy Protocol también incluye el ID del punto de enlace. Esta información se codifica mediante un vector de tipo-longitud-valor (TLV), como se indica a continuación.

Campo	Longitud (en octetos)	Descripción
Tipo	1	PP2_TYPE_AWS (0xEA)
Length	2	Longitud del valor
Valor	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	Variable (longitud del valor menos 1)	ID del punto de conexión

Para ver un ejemplo que analiza el tipo 0xEA de TLV, consulte https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot.

Habilitar Proxy Protocol

Antes de habilitar Proxy Protocol en un grupo de destino, asegúrese de que sus aplicaciones esperan e encabezado Proxy Protocol v2 y pueden analizarlo. De lo contrario, es posible que se produzca un error. Para obtener más información, consulte el documento sobre las versiones 1 y 2 del protocolo PROXY.

Console

Para habilitar el protocolo proxy, versión 2

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 abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la página Editar atributos, seleccione Proxy Protocol v2.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar el protocolo proxy, versión 2

Utilice el comando modify-target-group-attributes con el atributo `proxy_protocol_v2.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=proxy_protocol_v2.enabled,Value=true"
```

CloudFormation

Para habilitar el protocolo proxy, versión 2

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir el atributo `proxy_protocol_v2.enabled`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "proxy_protocol_v2.enabled"
          Value: "true"
```

Sesiones rápidas

Las sesiones rápidas son un mecanismo para direccionar el tráfico de clientes al mismo destino en un grupo de destino. Resulta útil para los servidores que mantienen información de estado, para ofrecer una experiencia de continuidad a los clientes.

Consideraciones

- El uso de sesiones rápidas puede provocar una distribución desigual de las conexiones y los flujos, lo que podría afectar a la disponibilidad de los destinos. Por ejemplo, todos los clientes situados

detrás del mismo dispositivo NAT tienen la misma dirección IP de origen. Por lo tanto, todo el tráfico de estos clientes se dirige al mismo destino.

- El balanceador de carga puede restablecer las sesiones rápidas de un grupo de destino si cambia el estado de alguno de sus destinos o si registra o anula el registro de destinos con el grupo de destino.
- Cuando el atributo de persistencia está activado para un grupo de destino, no se admiten las comprobaciones de estado pasivas. Para obtener más información, consulte Comprobaciones de estado de los grupos de destino.
- Las sesiones persistentes no son compatibles con los oyentes TLS ni QUIC.

Console

Para habilitar las sesiones persistentes

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 abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En la configuración de selección de destinos, active Persistencia.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar las sesiones persistentes

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

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=stickiness.enabled,Value=true"
```

CloudFormation

Para habilitar las sesiones persistentes

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir el atributo `stickiness.enabled`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "stickiness.enabled"
          Value: "true"
```

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 se puede utilizar 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 red, el equilibrio de carga entre zonas está desactivado de forma predeterminada a nivel del equilibrador de carga, pero puede habilitarlo en cualquier momento. En el caso de los grupos de destino, el valor predeterminado consiste en usar la configuración del equilibrador de carga; no obstante, puede reemplazar ese valor predeterminado al habilitar o desactivar explícitamente el equilibrio de carga entre zonas a nivel del grupo de destino.

Consideraciones

- Cuando se habilita el equilibrio de carga entre zonas para un equilibrador de carga de red, se aplican cargos por transferencia de datos de EC2. Para obtener más información, consulte Descripción de los cargos por transferencia de datos en la Guía del usuario de exportación de datos de AWS

- La configuración del grupo de destino determina el comportamiento del equilibrio de carga del grupo de destino. Por ejemplo, si el equilibrio de carga entre zonas está habilitado en el nivel del equilibrador de carga y deshabilitado en el nivel del grupo de destino, el tráfico enviado al grupo de destino no se enruta a través de las zonas de disponibilidad.
- Cuando el equilibrio de carga entre zonas está desactivado, asegúrese de contar con capacidad suficiente de destinos en cada una de las zonas de disponibilidad del equilibrador de carga, de modo que cada zona pueda atender su carga de trabajo asociada.
- Cuando el equilibrio de carga entre zonas está desactivado, asegúrese de que todos los grupos de destino participen en las mismas zonas de disponibilidad. Una zona de disponibilidad vacía se considera en mal estado.
- Puede habilitar o desactivar el equilibrio de carga entre zonas a nivel del grupo de destino si el tipo de grupo de destino es `instance` o `ip`. Si el tipo de grupo de destino es `alb`, el grupo de destino siempre hereda la configuración del equilibrio de carga entre zonas del equilibrador de carga.

Para obtener más información sobre cómo habilitar el equilibrio de carga entre zonas a nivel del equilibrador de carga, consulte the section called “Balance de carga entre zonas”.

Console

Para habilitar el equilibrio de carga entre zonas para un grupo de destino

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en 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 Activado para el Equilibrio de carga entre zonas.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar el equilibrio de carga entre zonas para un grupo de destino

Utilice el comando modify-target-group-attributes con el atributo `load_balancing.cross_zone.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Para habilitar el equilibrio de carga entre zonas para un grupo de destino

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir el atributo `load_balancing.cross_zone.enabled`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Interrupción de la conexión para destinos en mal estado

La interrupción de la conexión está habilitada de manera predeterminada. De manera predeterminada, cuando el destino de un equilibrador de carga de red no supera las comprobaciones de estado configuradas y se considera que está en mal estado, el equilibrador de carga finaliza las conexiones establecidas y deja de enrutar nuevas conexiones hacia el destino. Si la finalización de conexiones está deshabilitada, el destino sigue considerándose en mal estado y no recibe nuevas conexiones, pero las conexiones establecidas se mantienen activas, lo que permite que se cierren sin problemas.

La terminación de conexiones para destinos en mal estado se configura a nivel del grupo de destino.

Console

Para modificar el atributo de terminación de conexiones

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. En la sección Gestión del estado defectuoso del destino, seleccione si desea activar o desactivar la opción Interrumpir las conexiones cuando los destinos no estén en buen estado.
6. Seleccione Save changes (Guardar cambios).

AWS CLI

Para desactivar el atributo de terminación de conexiones

Utilice el comando modify-target-group-attributes con el atributo `target_health_state.unhealthy.connection_termination.enabled`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.connection_termination.enabled,Value=false"
```

CloudFormation

Para desactivar el atributo de terminación de conexiones

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir el atributo `target_health_state.unhealthy.connection_termination.enabled`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
```

```
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.connection_termination.enabled"
          Value: "false"
```

Intervalo de drenaje para destinos en mal estado

Los destinos con el estado `unhealthy.draining` se consideran en mal estado y no reciben nuevas conexiones, pero retienen las conexiones establecidas durante el intervalo configurado. El intervalo de conexión en mal estado indica cuánto tiempo permanece un destino en `unhealthy.draining` estado antes de volver a estar en `unhealthy`. Si el destino supera las comprobaciones de estado durante el intervalo de conexión en mal estado, el sistema restablece su estado a `healthy`. Si se desencadena una anulación del registro, el estado del destino pasa a ser `draining` y comienza el tiempo de espera de la anulación del registro.

Requisito

La finalización de conexiones debe estar deshabilitada para poder habilitar el intervalo de drenaje para destinos en mal estado.

Console

Para modificar el intervalo de drenaje de destinos en mal estado

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. En la sección Administración de estados en mal estado del destino, asegúrese de que la opción Terminar conexiones en destinos en mal estado esté desactivada.
6. Introduzca un valor en Intervalo de drenaje para destinos en mal estado.
7. Seleccione Save changes (Guardar cambios).

AWS CLI

Para modificar el intervalo de drenaje de destinos en mal estado

Utilice el comando modify-target-group-attributes con el atributo `target_health_state.unhealthy.draining_interval_seconds`.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.draining_interval_seconds,Value=60"
```

CloudFormation

Para modificar el intervalo de drenaje de destinos en mal estado

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir el atributo `target_health_state.unhealthy.draining_interval_seconds`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.draining_interval_seconds"
          Value: "60"
```

Registro de destinos del equilibrador de carga de red

Cuando el destino esté preparado para controlar solicitudes, lo registra con uno o más grupos de destino. El tipo de destino del grupo de destino determina cómo se registran los destinos. Por ejemplo, puede registrar los ID de instancia, las direcciones IP o un equilibrador de carga de aplicación. El equilibrador de carga de red comienza a direccionar las solicitudes a los destinos tan pronto como se completa el proceso de registro y el destino supera las comprobaciones de estado iniciales. El proceso de registro puede tardar unos minutos en completarse y comenzar las comprobaciones de estado. Para obtener más información, consulte Comprobaciones de estado de grupos de destino del equilibrador de carga de red.

Si la demanda aumenta en los destinos registrados actualmente, puede registrar más para controlar esa demanda. Si la demanda baja en los destinos registrados, puede anular el registro de los destinos en el grupo de destino. El proceso de anulación de registro puede tardar unos minutos en completarse y que el balanceador de carga detenga las solicitudes de enrutamiento al destino. Si la demanda aumenta posteriormente, puede registrar de nuevo los destinos a los que anuló el registro con el grupo de destino. Si necesita dar servicio a un destino, puede anular el registro y volver a registrarlo cuando se complete el servicio.

Cuando se anula el registro de un destino, Elastic Load Balancing 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. Una vez completada la anulación del registro, el estado del destino cambia a `unused`. Para obtener más información, consulte Retardo de anulación del registro.

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 equilibrador de carga 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.

Contenido

Grupos de seguridad de destino

Antes de agregar destinos al grupo de destino, configure los grupos de seguridad asociados a los destinos para que acepten el tráfico de su equilibrador de carga de red.

Recomendaciones para los grupos de seguridad de destino si el equilibrador de carga tiene un grupo de seguridad asociado

- Para permitir el tráfico de clientes: agregue una regla que haga referencia al grupo de seguridad asociado al equilibrador de carga.
- Para permitir el tráfico de PrivateLink: si configuró el equilibrador de carga para evaluar las reglas de entrada del tráfico que se envía a través de AWS PrivateLink, agregue una regla que acepte el tráfico del grupo de seguridad del equilibrador de carga en el puerto de tráfico. De lo contrario, agregue una regla que acepte el tráfico de las direcciones IP privadas del equilibrador de carga en el puerto de tráfico.
- Para aceptar las comprobaciones de estado del equilibrador de carga: agregue una regla que acepte el tráfico de comprobaciones de estado de los grupos de seguridad del equilibrador de carga en el puerto de comprobación de estado.

Recomendaciones para los grupos de seguridad de destino si el equilibrador de carga no tiene un grupo de seguridad asociado

- Para permitir el tráfico de clientes: si el equilibrador de carga conserva las direcciones IP de los clientes, agregue una regla que acepte el tráfico de las direcciones IP de los clientes aprobados en el puerto de tráfico. De lo contrario, agregue una regla que acepte el tráfico de las direcciones IP privadas del equilibrador de carga en el puerto de tráfico.
- Para permitir el tráfico de PrivateLink: agregue una regla que acepte el tráfico de las direcciones IP privadas del equilibrador de carga en el puerto de tráfico.
- Para aceptar las comprobaciones de estado del equilibrador de carga: agregue una regla que acepte el tráfico de comprobaciones de estado de las direcciones IP privadas del equilibrador de carga en el puerto de comprobación de estado.

Cómo funciona la preservación de la IP del cliente

Los equilibradores de carga de red no conservan las direcciones IP de los clientes a menos que se establezca el atributo `preserve_client_ip.enabled` en `true`. Además, con equilibradores de carga de red de pila doble, la conservación de la dirección IP del cliente no funciona cuando se traducen direcciones IPv4 a IPv6 o IPv6 a IPv4. La conservación de la dirección IP del cliente solo funciona cuando las direcciones IP del cliente y del destino son ambas IPv4 o ambas IPv6.

Para buscar las direcciones IP privadas del equilibrador de carga mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Network Interfaces.
3. En el campo de búsqueda, escriba el nombre de su equilibrador de carga de red. Hay una interfaz de red por cada subred de balanceador de carga.
4. En la pestaña Detalles de cada interfaz de red, copie la dirección desde Dirección IPv4 privada.

Para obtener más información, consulte Actualización de los grupos de seguridad del equilibrador de carga de red.

ACL de red

Cuando se registran instancias EC2 como destinos, es preciso asegurarse de que las ACL de red de las subredes de las instancias permitan el tráfico tanto en el puerto del agente de escucha como en el puerto de comprobación de estado. La lista de control de acceso (ACL) de red predeterminada de una VPC permite todo el tráfico de entrada y salida. Si crea ACL de red personalizadas, compruebe que permiten el tráfico correspondiente.

Las ACL de red asociadas a las subredes de las instancias deben permitir el siguiente tráfico para un equilibrador de carga con acceso a Internet.

Reglas recomendadas para subredes de instancia

Inbound

Origen	Protocolo	Rango de puertos	Comment
Direcciones IP de clientes	*agente de escucha*	*puerto de destino*	Allow client traffic (IP Preservation: ON)
CIDR de VPC	*oyente*	*puerto de destino*	Allow client traffic (IP Preservation: OFF)
CIDR de VPC	*comprobación de estado*	*comprobación de estado*	Allow health check traffic

Outbound

Destino	Protocolo	Rango de puertos	Comment
Direcciones IP de clientes	*agente de escucha*	1024-65535	Allow return traffic to client (IP Preservation: ON)
CIDR de VPC	*oyente*	1024-65535	Allow return traffic to client (IP Preservation: OFF)
CIDR de VPC	*comprobación de estado*	1024-65535	Allow health check traffic

Las ACL de red asociadas a las subredes del equilibrador de carga deben permitir el siguiente tráfico para un equilibrador de carga con acceso a Internet.

Reglas recomendadas para subredes de balanceador de carga

Inbound

Origen	Protocolo	Rango de puertos	Comment
Direcciones IP de clientes	*agente de escucha*	*agente de escucha*	Allow client traffic
CIDR de VPC	*oyente*	1024-65535	Allow response from target
CIDR de VPC	*comprobación de estado*	1024-65535	Allow health check traffic

Outbound

Destino	Protocolo	Rango de puertos	Comment
Direcciones IP de clientes	*agente de escucha*	1024-65535	Allow responses to clients
CIDR de VPC	*oyente*	*puerto de destino*	Allow requests to targets

CIDR de VPC	*comprobación de estado*	*comprobación de estado*	Allow health check to targets

En el caso de un equilibrador de carga interno, las ACL de red de las subredes de las instancias y los nodos del equilibrador de carga deben permitir el tráfico entrante y saliente hacia y desde el CIDR de la VPC, en el puerto de oyente y en los puertos efímeros.

Subredes compartidas

Los participantes pueden crear un equilibrador de carga de red en una VPC compartida. Los participantes no pueden registrar un destino que se ejecute en una subred que no esté compartida con ellos.

Se admiten las subredes compartidas para los equilibradores de carga de red en todas las regiones de AWS, excepto:

- Asia-Pacífico (Osaka) `ap-northeast-3`
- Asia-Pacífico (Hong Kong) `ap-east-1`
- Medio Oriente (Baréin) `me-south-1`
- AWS China (Pekín) `cn-north-1`
- AWS China (Ningxia) `cn-northwest-1`

Cómo registrar destinos

Cada grupo de destino debe tener al menos un destino registrado en cada zona de disponibilidad que esté habilitado para el equilibrador de carga.

El tipo de destino del grupo de destino determina qué destinos puede registrar. Para obtener más información, consulte Tipo de destino. Utilice la información siguiente para registrar destinos con un grupo de destino de tipo `instance` o `ip`. Si el tipo de destino es `alb`, consulte Uso de equilibradores de carga de aplicación como destinos.

Requisitos y consideraciones

- Una instancia debe tener el estado `running` al registrarla.
- No puede registrar instancias por ID de instancia si usa uno de los siguientes tipos de instancia: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1.

- Al registrar destinos por ID de instancia, las instancias deben estar en la misma VPC que el equilibrador de carga de red. No puede registrar instancias por ID de instancia si están en una VPC interconectada a la VPC del equilibrador de carga (misma región o región diferente). Puede registrar estas instancias por dirección IP.
- Al registrar los destinos por ID de instancia para un grupo de destinos de IPv6, los destinos deben tener una dirección IPv6 principal asignada. Para obtener más información, consulte Direcciones IPv6 en la Guía del usuario de Amazon EC2
- Al registrar destinos por dirección IP para un grupo de destinos IPv4, las direcciones IP que registre deben pertenecer a uno de los siguientes bloques de CIDR:
  - Las subredes de la VPC del grupo de destinos
  - 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)
- Al registrar destinos por dirección IP para un grupo de destinos IPv6, las direcciones IP que registre deben estar dentro del bloque de CIDR IPv6 de la VPC o dentro del bloque de CIDR IPv6 de una VPC emparejada.
- Si registra un destino por dirección IP y la dirección IP está en la misma VPC que el balanceador de carga, el balanceador de carga verifica que proviene de una subred a la que tiene acceso.
- En el caso de los grupos de destino UDP, TCP_UDP, QUIC y TCP_QUIC, no registre instancias por dirección IP si residen fuera de la VPC del equilibrador de carga o si utilizan alguno de los siguientes tipos de instancia: C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 o T1. Es posible que los destinos que residen fuera de la VPC del equilibrador de carga o que usen un tipo de instancia no compatible puedan recibir tráfico del equilibrador de carga, pero luego no puedan responder.

Requisitos y consideraciones específicas de QUIC

- Todos los destinos registrados en un grupo de destino QUIC o TCP_QUIC deben tener un ID de servidor especificado.
- Los ID de servidor deben ser únicos para todos los destinos que existan dentro de un oyente de un equilibrador de carga de red.
- Los ID de servidor QUIC siempre tienen 8 bytes. Al registrar un destino, el ID de servidor debe tener el formato `0x` seguido de 16 caracteres hexadecimales.

- Una vez que un destino se registra con un ID de servidor, dicho ID es inmutable. Para cambiar el ID de servidor de un destino, primero se debe anular su registro y, a continuación, registrarse de nuevo con el nuevo ID de servidor.
- Cada combinación de identificador de destino y puerto debe tener un único ID de servidor. No se admite el uso de un ID de servidor diferente para la misma combinación de dirección IP o ID de instancia y puerto dentro de la misma VPC.
- Evite reutilizar el mismo ID de servidor para un destino distinto dentro de un plazo de 6 horas.

Console

Para registrar destinos

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. Elija Register targets (Registrar destino).
6. Si el tipo de destino del grupo de destinos es `instance`, seleccione las instancias disponibles, anule el puerto predeterminado si es necesario y, posteriormente, elija Incluir como pendientes a continuación.
7. Si el tipo de destino del grupo de destino es `ip`, para cada dirección IP, seleccione la red, introduzca la dirección IP y los puertos, y seleccione Incluir como pendientes a continuación.
8. Si el tipo de destino del grupo de destino es `alb`, modifique el puerto predeterminado si es necesario y seleccione el equilibrador de carga de aplicaciones. Para obtener más información, consulte Uso de equilibradores de carga de aplicación como destinos.
9. Si el protocolo del grupo de destino es QUIC o TCP_QUIC, asegúrese de que se haya especificado un ID de servidor.
10. Seleccione Registrar destinos pendientes.

AWS CLI

Para registrar destinos

Use el comando register-targets. El siguiente ejemplo registra destinos por ID de instancia. Dado que no se especifica el puerto, el equilibrador de carga utiliza el puerto del grupo de destinos.

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

El siguiente ejemplo registra destinos por dirección IP. Dado que no se especifica el puerto, el equilibrador de carga utiliza el puerto del grupo de destinos.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10 Id=10.0.50.20
```

En el siguiente ejemplo, se registra un equilibrador de carga de aplicaciones como destino.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=application-load-balancer-arn
```

En el siguiente ejemplo, se registra destinos en un grupo de destino QUIC o TCP_QUIC.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10,QuicServerId=0xa1b2c3d4e5f65890
 Id=10.0.50.20,QuicServerId=0xa1b2c3d4e5f65999
```

CloudFormation

Para registrar destinos

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir los nuevos destinos. En el siguiente ejemplo, se registran dos destinos por ID de instancia.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
```

```
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
```

En el siguiente ejemplo, se registran dos destinos por ID de instancia en un grupo de destino con protocolo QUIC o TCP_QUIC.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65999
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
          QuicServerId: 0xa1b2c3d4e5f65000
```

Anulación del registro del destino

Si la demanda de la aplicación se reduce o si 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 balanceador de carga deja de direccionar el tráfico a un destino tan pronto como se anula su registro. El destino adquiere el estado `draining` hasta que se completan las solicitudes en tránsito.

Console

Para anular el registro de destinos

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, seleccione los destinos que desea eliminar.
5. Elija Anular registro.

AWS CLI

Para anular el registro de destinos

Use el comando deregister-targets. El siguiente ejemplo anula el registro de dos destinos que se registraron por ID de instancia.

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

Utilice un equilibrador de carga de aplicaciones como destino de un equilibrador de carga de red

Puede crear un grupo de destino con un único equilibrador de carga de aplicación como destino y configurar el equilibrador de carga de red para que le redirija el tráfico. En este escenario, el equilibrador de carga de aplicación asume la decisión de equilibrio de carga en cuanto llega el tráfico. Esta configuración combina las funciones de ambos equilibradores de carga y ofrece las siguientes ventajas:

- Puede usar la característica de enrutamiento basado en solicitudes de capa 7 del equilibrador de carga de aplicación en combinación con las características que admite el equilibrador de carga de red, como los servicios de punto de conexión (AWS PrivateLink) y las direcciones IP estáticas.
- Puede usar esta configuración para aplicaciones que necesitan un único punto de conexión para varios protocolos, como los servicios multimedia que utilizan HTTP para la señalización y RTP para transmitir contenido.

Puede utilizar esta característica con un equilibrador de carga de aplicación interno o con acceso a Internet como destino de un equilibrador de carga de red interno o con acceso a Internet.

Consideraciones

- Solo puede registrar un equilibrador de carga de aplicaciones por grupo de destino.
- Para asociar un equilibrador de carga de aplicaciones como destino de un equilibrador de carga de red, ambos equilibradores de carga deben estar en la misma VPC y dentro de la misma cuenta.
- Puede asociar un equilibrador de carga de aplicaciones como destino de hasta dos equilibradores de carga de red. Para ello, registre el equilibrador de carga de aplicaciones en un grupo de destino independiente para cada equilibrador de carga de red.
- Cada equilibrador de carga de aplicaciones que registre en un equilibrador de carga de red reduce en 50 el número máximo de destinos por zona de disponibilidad para ese equilibrador de carga de red. Puede deshabilitar la equilibración de carga entre zonas en ambos equilibradores de carga para minimizar la latencia y evitar los cargos por transferencia de datos regionales. Para obtener más información, consulte Cuotas para los equilibradores de carga de red.
- Si el tipo de grupo de destino es `alb`, no puede modificar los atributos del grupo de destino. Estos atributos siempre utilizan los valores predeterminados.
- Después de registrar un equilibrador de carga de aplicación como destino, no podrá eliminar el equilibrador de carga de aplicación hasta que anule el registro de todos los grupos de destino.
- La comunicación entre un equilibrador de carga de red y un equilibrador de carga de aplicaciones siempre utiliza IPv4.

Tareas

- Requisito previo
- Paso 1: Creación de un grupo de destino de tipo alb
- Paso 2: Creación de un equilibrador de carga de red y configuración del enrutamiento
- Paso 3: (opcional) crear un servicio de punto de conexión de VPC

Requisito previo

Si aún no tiene un equilibrador de carga de aplicaciones para usarlo como destino, cree el equilibrador de carga, sus oyentes y sus grupos de destino. Para obtener más información, consulte Crear un Equilibrador de carga de aplicación en la Guía del usuario para Equilibradores de carga de aplicación.

Paso 1: Creación de un grupo de destino de tipo alb

Cree un grupo de destino de tipo `alb`. Puede registrar el equilibrador de carga de aplicaciones como destino al crear el grupo de destino o más adelante.

Console

Para crear un grupo de destino para un equilibrador de carga de aplicaciones como destino

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 el panel Configuración básica, en Elegir un tipo de destino, seleccione Equilibrador de carga de aplicaciones.
5. En Nombre del grupo de destino, escriba el nombre del grupo de destino.
6. En Protocolo, solo se permite el TCP. Seleccione el Puerto para su grupo de destino. El puerto de este grupo de destino debe coincidir con el puerto del oyente del equilibrador de carga de aplicaciones. Si elige un puerto distinto para este grupo de destino, puede actualizar el puerto del oyente del equilibrador de carga de aplicaciones para que coincida.
7. En VPC, seleccione la nube privada virtual (VPC) para el grupo de destino. Debe ser la misma VPC que utiliza el equilibrador de carga de aplicaciones.
8. En Comprobaciones de estado, elija HTTP o HTTPS como el Protocolo de comprobación de estado. Las comprobaciones de estado se envían al equilibrador de carga de aplicación y se reenvían a sus destinos mediante el puerto, el protocolo y la ruta de ping especificados. Asegúrese de que su equilibrador de carga de aplicación pueda recibir estas comprobaciones de estado mediante un oyente con un puerto y un protocolo que coincidan con el puerto y el protocolo de la comprobación de estado.
9. (Opcional) Amplíe las Etiquetas. Para cada etiqueta, seleccione Agregar nueva etiqueta e introduzca una clave de etiqueta y un valor de etiqueta.
10. Elija Siguiente.
11. Si ya está listo para registrar el equilibrador de carga de aplicaciones, seleccione Registrar ahora, modifique el puerto predeterminado si es necesario y seleccione el equilibrador de carga de aplicaciones. El equilibrador de carga de aplicaciones debe tener un oyente en el mismo puerto que el grupo de destino. Puede agregar o editar un oyente en este equilibrador

de carga para que coincida con el puerto del grupo de destino, o bien volver al paso anterior y cambiar el puerto del grupo de destino.

Si aún no está listo para registrar el equilibrador de carga de aplicaciones como destino, seleccione Registrar más adelante y registre el destino posteriormente. Para obtener más información, consulte the section called “Cómo registrar destinos”.

12. Elija Crear grupo de destino.

AWS CLI

Para crear un grupo de destino de tipo alb

Utilice el comando create-target-group. El protocolo debe ser TCP y el puerto debe coincidir con el puerto del oyente del equilibrador de carga de aplicaciones.

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type alb \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

CloudFormation

Para crear un grupo de destino de tipo alb

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::TargetGroup. El protocolo debe ser TCP y el puerto debe coincidir con el puerto del oyente del equilibrador de carga de aplicaciones.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: alb
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
```

```
      Targets:
        - Id: !Ref myApplicationLoadBalancer
          Port: 80
```

Paso 2: Creación de un equilibrador de carga de red y configuración del enrutamiento

Al crear el equilibrador de carga de red, puede configurar la acción predeterminada para reenviar el tráfico al equilibrador de carga de aplicaciones.

Console

Para crear el equilibrador de carga de red

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibrio de carga), elija Load Balancers (Equilibradores de carga).
3. Elija Crear un equilibrador de carga.
4. En Equilibrador de carga de red, elija Crear.
5. Configuración básica
   a. En Nombre del balanceador de carga, escriba un nombre para el equilibrador de carga de red.
   b. Para Scheme (Esquema), elija ya sea expuesto a internet o interno. Un equilibrador de carga de red expuesto a Internet enruta las solicitudes desde los clientes hasta los destinos a través de Internet. Un equilibrador de carga de red interno enruta las solicitudes hacia los destinos mediante direcciones IP privadas.
   c. En Tipo de dirección IP del equilibrador de carga, seleccione IPv4 si los clientes usan direcciones IPv4 para comunicarse con el equilibrador de carga de red, o Doble pila si los clientes usan tanto direcciones IPv4 como IPv6 para comunicarse con el equilibrador de carga de red.
6. Asignación de redes
   a. En VPC, seleccione la misma VPC que utilizó para el equilibrador de carga de aplicaciones. Cuando se utiliza un equilibrador de carga de acceso a Internet, solo se pueden seleccionar VPC que tengan una puerta de enlace de Internet.

b. En Zonas de disponibilidad y subredes, seleccione al menos una zona de disponibilidad y una subred por zona. Recomendamos seleccionar las mismas zonas de disponibilidad que están habilitadas para el equilibrador de carga de aplicaciones. Esto optimiza la disponibilidad, el escalado y el rendimiento.

   (Opcional) Para usar direcciones IP estáticas, elija Usar una dirección IP elástica en la configuración de IPv4 de cada zona de disponibilidad. Con las direcciones IP estáticas, puede agregar determinadas direcciones IP a una lista de direcciones IP permitidas para los firewalls o puede usar una codificación rígida para direcciones IP de clientes.

7. Grupos de seguridad

   Preseleccionamos el grupo de seguridad predeterminado para la VPC del equilibrador de carga. Puede seleccionar grupos de seguridad adicionales según sea necesario. Si no tiene un grupo de seguridad que cumpla con sus requisitos, elija crear un nuevo grupo de seguridad para crearlo ahora. Para obtener más información, consulte Crear un grupo de seguridad en la Guía del usuario de Amazon VPC.

   > **Warning**
   >
   > Si no asocia ahora ningún grupo de seguridad al equilibrador de carga de red, no podrá asociarlo más adelante.

   > **Warning**
   >
   > Para utilizar oyentes QUIC o TCP_QUIC, el equilibrador de carga de red no debe tener grupos de seguridad.

8. Los oyentes y el enrutamiento

   a. De forma predeterminada, el oyente acepta tráfico de TCP en el puerto 80. Solo los oyentes de TCP pueden reenviar el tráfico a un grupo de destino del equilibrador de carga de aplicación. Debe mantener el Protocolo como TCP, pero puede modificar el Puerto según sea necesario.

      Con esta configuración, puede usar oyentes HTTPS en el equilibrador de carga de aplicación para interrumpir el tráfico TLS.

   b. En Acción predeterminada, seleccione el grupo de destino que creó en el paso anterior.

c. (Opcional) Elija Agregar etiqueta del oyente e introduzca una clave de etiqueta y un valor de etiqueta.

9. Etiquetas del equilibrador de carga

   (Opcional) Amplíe Etiquetas del equilibrador de carga. Elija Agregar nueva etiqueta e introduzca una clave de etiqueta y un valor de etiqueta. Para obtener más información, consulte Etiquetas.

10. Resumen

    Revise la configuración y seleccione Crear equilibrador de carga.

AWS CLI

Para crear el equilibrador de carga de red

Utilice el comando create-load-balancer. Recomendamos que utilice las mismas zonas de disponibilidad que están habilitadas para el equilibrador de carga de aplicaciones.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Para agregar un oyente TCP

Utilice el comando create-listener para agregar un oyente TCP. Solo los oyentes TCP pueden reenviar tráfico a un equilibrador de carga de aplicaciones. En la acción predeterminada, utilice el grupo de destino que creó en el paso anterior.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Para crear el equilibrador de carga de red

Defina un recurso de tipo AWS::ElasticLoadBalancingV2::LoadBalancer y un recurso de tipo AWS::ElasticLoadBalancingV2::Listener. Solo los oyentes TCP pueden reenviar tráfico a un equilibrador de carga de aplicaciones. En la acción predeterminada, utilice el grupo de destino que creó en el paso anterior.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-load-balancer
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup

  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Paso 3: (opcional) crear un servicio de punto de conexión de VPC

Para usar el equilibrador de carga de red que configuró en el paso anterior como punto de conexión para la conectividad privada, puede habilitar AWS PrivateLink. Con esto se establece una conexión privada a su equilibrador de carga como un servicio de punto de conexión.

Para crear un servicio de punto de conexión de VPC mediante el equilibrador de carga de red

1. En el panel de navegación, seleccione Load Balancers.
2. Seleccione el nombre del equilibrador de carga de red para abrir la página de detalles.
3. En la pestaña Integraciones, expanda Servicios de punto de conexión de VPC (AWS PrivateLink).

4. Elija Crear servicios de punto de conexión para abrir la página Servicios de punto de conexión. Para ver los pasos restantes, consulte Crear un servicio de punto de conexión en la Guía AWS PrivateLink.

Etiquetado de un grupo de destino para el equilibrador de carga de red

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

Console

Para administrar las etiquetas de un grupo de destino

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (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. Seleccione Save changes (Guardar cambios).

AWS CLI

Para agregar etiquetas de

Utilice el comando add-tags. En el siguiente ejemplo, se agregan dos etiquetas.

```
aws elbv2 add-tags \
    --resource-arns target-group-arn \
    --tags "Key=project,value=lima" "Key=department,Value=digital-media"
```

Para eliminar etiquetas

Utilice el comando remove-tags. En el siguiente ejemplo, se eliminan las etiquetas con las claves especificadas.

```
aws elbv2 remove-tags \
    --resource-arns target-group-arn \
    --tag-keys project department
```

CloudFormation

Para agregar etiquetas de

Actualice el recurso AWS::ElasticLoadBalancingV2::TargetGroup para incluir la propiedad `Tags`.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
```

```
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Eliminación de un grupo de destino del equilibrador de carga de red

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.

Console

Para eliminar un grupo de destino

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el grupo de destino y elija Actions, Delete.
4. Elija Eliminar.

AWS CLI

Para eliminar un grupo de destino

Utilice el comando delete-target-group.

```
aws elbv2 delete-target-group \
    --target-group-arn target-group-arn
```

Monitorizar los equilibradores de carga de red

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.

Métricas de CloudWatch

Puede utilizar Amazon CloudWatch para recuperar estadísticas sobre los puntos de datos de los equilibradores de carga y destinos en conjuntos ordenados de datos de serie temporal denominados métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte Métricas de CloudWatch para el equilibrador de carga de red.

Logs de flujo de VPC

Puede utilizar registros de flujo de VPC para capturar información detallada sobre el tráfico entrante y saliente del equilibrador de carga de red. Para obtener más información, consulte Registros de flujo de VPC en la Guía del usuario de Amazon VPC.

Cree un log de flujo para cada interfaz de red del balanceador de carga. Hay una interfaz de red por cada subred de balanceador de carga. Para identificar las interfaces de red de un equilibrador de carga de red, busque el nombre del equilibrador de carga en el campo de descripción de la interfaz de red.

Existen dos entradas para cada conexión a través de su equilibrador de carga de red, una para la conexión frontend entre el cliente y el equilibrador de carga y la otra para la conexión backend entre el equilibrador de carga y el destino. Si el atributo de preservación de la IP del cliente del grupo de destino está habilitado, la conexión aparece en la instancia como una conexión desde el cliente. De lo contrario, la IP de origen de la conexión es la dirección IP privada del equilibrador de carga. Si el grupo de seguridad de la instancia no permite conexiones desde el cliente pero las ACL de red de la subred del balanceador de carga sí las permiten, los logs de la interfaz de red del balanceador de carga muestran "ACCEPT OK" para las conexiones frontend y backend, mientras que los logs de la interfaz de red de la instancia muestran "REJECT OK" para la conexión.

Si un equilibrador de carga de red tiene grupos de seguridad asociados, los registros de flujo contienen entradas para el tráfico permitido o rechazado por los grupos de seguridad. En el caso de los equilibradores de carga de red con oyentes de TLS, las entradas de los registros de flujo reflejan solo las entradas rechazadas.

Amazon CloudWatch Internet Monitor

Puede usar Internet Monitor para tener visibilidad sobre cómo los problemas de Internet afectan al rendimiento y la disponibilidad entre las aplicaciones alojadas en AWS y los usuarios finales. También puede explorar, casi en tiempo real, cómo mejorar la latencia prevista de su aplicación pasando a utilizar otros servicios o redirigiendo el tráfico a su carga de trabajo a través de diferentes Regiones de AWS. Para obtener más información, consulte Uso de Amazon CloudWatch Internet Monitor.

Registros de acceso

Puede usar registros de acceso para capturar información detallada sobre las solicitudes de TLS enviadas al balanceador de carga. Los archivos de registro están almacenados 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 para el equilibrador de carga de red.

Registros de CloudTrail

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 utilizar estos registros de CloudTrail para determinar qué llamadas se han efectuado, la dirección IP de origen de la que procede la llamada, quién la ha realizado, cuándo, etc. Para obtener más información, consulte Registro de llamadas a la API para Elastic Load Balancing mediante CloudTrail.

Métricas de CloudWatch para el equilibrador de carga de red

Elastic Load Balancing publica puntos de datos en Amazon CloudWatch sobre los equilibradores de carga y los destinos. CloudWatch permite recuperar las estadísticas sobre estos puntos de datos como un conjunto ordenado de datos de serie temporal denominado 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 alarma de CloudWatch para monitorizar una métrica determinada e iniciar una acción (por ejemplo, enviar una notificación a una dirección de correo electrónico) si la métrica no está comprendida dentro del intervalo que considera aceptable.

Elastic Load Balancing únicamente notifica las métricas a CloudWatch mientras las solicitudes están fluyendo a través del equilibrador 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. En el caso de los equilibradores de carga de red con grupos de seguridad, el tráfico rechazado por los grupos de seguridad no se captura en las métricas de CloudWatch.

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

Contenido

Métricas del balanceador de carga de red

El espacio de nombres de `AWS/NetworkELB` incluye las siguientes métricas.

Métrica	Descripción
`ActiveFlowCount`	Número total de flujos (o conexiones) simultáneos de clientes a destinos. Esta métrica incluye las conexiones cuyo estado sea SYN_SENT o ESTABLISHED. Las conexiones TCP no se terminan en el balanceador de carga, por lo que un cliente que abre una conexión TCP con un destino se contabiliza como un solo flujo. Criterios del informe: se informa siempre. Estadísticas: las estadísticas más útiles son `Average`, `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`

Métrica	Descripción
`ActiveFlowCount_TCP`	Número total de flujos (o conexiones) TCP simultáneos de clientes a destinos. Esta métrica incluye las conexiones cuyo estado sea SYN_SENT o ESTABLISHED. Las conexiones TCP no se terminan en el balanceador de carga, por lo que un cliente que abre una conexión TCP con un destino se contabiliza como un solo flujo. Criterios del informe: hay un valor distinto de cero Estadísticas: las estadísticas más útiles son `Average`, `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`
`ActiveFlowCount_TLS`	Número total de flujos (o conexiones) TLS simultáneos de clientes a destinos. Esta métrica incluye las conexiones cuyo estado sea SYN_SENT o ESTABLISHED. Criterios del informe: hay un valor distinto de cero. Estadísticas: las estadísticas más útiles son `Average`, `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`

Métrica	Descripción
`ActiveFlowCount_UDP`	Número total de flujos (o conexiones) UDP simultáneos de clientes a destinos. Criterios del informe: hay un valor distinto de cero. Estadísticas: las estadísticas más útiles son `Average`, `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer` • `TargetGroup`
`ActiveZonalShiftHostCount`	Número de destinos que están participando activamente en el cambio de zona actualmente. Criterios de notificación: se notifica cuando el equilibrador de carga opta por el cambio de zona. Estadísticas: las estadísticas más útiles son `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`ClientTLSNegotiationErrorCount`	Número total de protocolos de enlace TLS que no se han superado durante la negociación entre un cliente y un agente de escucha TLS. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer`

Métrica	Descripción
`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`
`ConsumedLCUs_TCP`	El número de unidades de capacidad del balanceador de carga (LCU) usadas por el balanceador de carga para TCP. Se paga por el número de LCU usadas a la hora. Para obtener más información, consulte Precios de Elastic Load Balancing. Criterios del informe: hay un valor distinto de cero. Estadísticas: todas Dimensiones • `LoadBalancer`
`ConsumedLCUs_TLS`	El número de unidades de capacidad del balanceador de carga (LCU) usadas por el balanceador de carga para TLS. Se paga por el número de LCU usadas a la hora. Para obtener más información, consulte Precios de Elastic Load Balancing. Criterios del informe: hay un valor distinto de cero. Estadísticas: todas Dimensiones • `LoadBalancer`

Métrica	Descripción
ConsumedLCUs_UDP	El número de unidades de capacidad del balanceador de carga (LCU) usadas por el balanceador de carga para UDP. Se paga por el número de LCU usadas a la hora. Para obtener más información, consulte Precios de Elastic Load Balancing. Criterios del informe: hay un valor distinto de cero. Estadísticas: todas Dimensiones • LoadBalancer
HealthyHostCount	El número de destinos que se considera que están en buen estado. Esta métrica no incluye ningún equilibrador de carga de aplicación registrado como destino. Criterios de notificación: se notifica si hay destinos registrados. Estadísticas: las estadísticas más útiles son Maximum y Minimum. Dimensiones • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
NewFlowCount	Número total de flujos (o conexiones) nuevos establecidos desde los clientes a los destinos en el periodo indicado. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup

Métrica	Descripción
NewFlowCount_TCP	Número total de flujos (o conexiones) TCP nuevos establecidos desde los clientes a los destinos en el periodo indicado. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup
NewFlowCount_TLS	Número total de flujos (o conexiones) TLS nuevos establecidos desde los clientes a los destinos en el periodo indicado. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup

Métrica	Descripción
NewFlowCount_UDP	Número total de flujos (o conexiones) UDP nuevos establecidos desde los clientes a los destinos en el periodo indicado. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer • TargetGroup
NewFlowCount_QUIC	El número total de datagramas UDP que requirieron una decisión de enrutamiento durante el periodo. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
PeakBytesPerSecond	El promedio más alto de bytes procesados por segundo, calculado cada 10 segundos durante el intervalo de muestreo. Esta métrica no incluye el tráfico de comprobación de estado. Criterios del informe: se informa siempre Estadísticas: la estadística más útil es Maximum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
PeakPacketsPerSecond	La velocidad media de paquetes más alta (paquetes procesados por segundo), calculada cada 10 segundos durante la ventana de muestreo. Esta métrica incluye el tráfico de comprobación de estado. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es `Maximum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
PortAllocationErrorCount	La cantidad total de errores efímeros de asignación de puertos durante una operación de traducción de IP de un cliente. Un valor distinto de cero indica que se han interrumpido las conexiones de los clientes. Nota: Los equilibradores de carga de red admiten 55 000 conexiones simultáneas o aproximadamente 55 000 conexiones por minuto a cada destino único (dirección IP y puerto) al realizar la traducción de direcciones de clientes. Para solucionar los errores de asignación de puertos, agregue más destinos al grupo de destino. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
ProcessedBytes	Número total de bytes procesados por el balanceador de carga, incluidos los encabezados TCP/IP. Este recuento incluye el tráfico entrante y saliente de los destinos, menos el tráfico de comprobación de estado. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes_TCP	Número total de bytes procesados por los agentes de escucha TCP. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes_TLS	Número total de bytes procesados por los agentes de escucha TLS. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
ProcessedBytes_UDP	Número total de bytes procesados por los agentes de escucha UDP. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes_QUIC	El número total de bytes procesados por los oyentes QUIC. Criterios del informe: hay un valor distinto de cero Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedPackets	La cantidad total de paquetes procesados por el equilibrador de carga. Este recuento incluye el tráfico entrante y saliente de los destinos, pero no el tráfico de comprobación de estado. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
`RejectedFlowCount`	Número total de flujos (o conexiones) rechazados por el equilibrador de carga. Criterios del informe: se informa siempre. Estadísticas: las estadísticas más útiles son `Average`, `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedFlowCount_TCP`	Número total de flujos (o conexiones) TCP rechazados por el equilibrador de carga. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ReservedLCUs`	El número de unidades de capacidad del equilibrador de carga (LCU) reservadas para el equilibrador de carga mediante la reserva de LCU. Criterios del informe: hay un valor distinto de cero Estadísticas: todas Dimensiones • `LoadBalancer`

Métrica	Descripción
SecurityGroupBlockedFlowCount_Inbound_ICMP	El número de mensajes ICMP nuevos rechazados por las reglas de entrada de los grupos de seguridad del equilibrador de cargas. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_TCP	La cantidad de flujos TCP nuevos rechazados por las reglas de entrada de los grupos de seguridad del equilibrador de cargas. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_UDP	La cantidad de flujos de UDP nuevos rechazados por las reglas de entrada de los grupos de seguridad del equilibrador de cargas. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
SecurityGroupBlockedFlowCount_Outbound_ICMP	La cantidad de mensajes ICMP nuevos rechazados por las reglas de salida de los grupos de seguridad del equilibrador de cargas. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_TCP	La cantidad de flujos TCP nuevos rechazados por las reglas de salida de los grupos de seguridad del equilibrador de cargas. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_UDP	La cantidad de flujos de UDP nuevos rechazados por las reglas de salida de los grupos de seguridad del equilibrador de cargas. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
`TargetTLSNegotiationErrorCount`	Número total de protocolos de enlace TLS que no se han superado durante la negociación entre un agente de escucha TLS y un destino. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer`
`TCP_Client_Reset_Count`	Número total de paquetes de restablecimiento (RST) enviados de un cliente a un destino. Estos restablecimientos los genera el cliente y los reenvía el balanceador de carga. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AavailabilityZone` , `LoadBalancer`
`TCP_ELB_Reset_Count`	El número total de paquetes de restablecimiento (RST) generados por el balanceador de carga. Para más información, consulte Solución de problemas. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrica	Descripción
TCP_Target_Reset_Count	Número total de paquetes de restablecimiento (RST) enviados de un destino a un cliente. Estos restablecimientos los genera el destino y los reenvía el balanceador de carga. Criterios del informe: se informa siempre. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
UnHealthyHostCount	El número de destinos que se considera que no están en buen estado. Esta métrica no incluye ningún equilibrador de carga de aplicación registrado como destino. Criterios de notificación: se notifica si hay destinos registrados. Estadísticas: las estadísticas más útiles son Maximum y Minimum. Dimensiones • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup
UnhealthyRoutingFlowCount	La cantidad de flujos (o conexiones) que se enrutan mediante la acción de conmutación por error de enrutamiento (apertura por error). Esta métrica no es compatible con oyentes TLS. Criterios del informe: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum.

Métrica	Descripción
`ZonalHealthStatus`	El número de zonas de disponibilidad que el equilibrador de carga considera en estado correcto. El equilibrador de carga emite un valor de 1 por cada zona de disponibilidad en estado correcto y un valor de 0 por cada zona de disponibilidad en estado no correcto. Criterios del informe: indica si se han activado las comprobaciones de estado. Estadísticas: las estadísticas más útiles son `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`QUIC_Unknown_Server_ID_Packet_Drop_Count`	El número de datagramas UDP descartados que contienen un ID de servidor que no está asociado a un destino en el equilibrador de carga de red. Criterios de generación de informes: se genera solo para oyentes QUIC. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Dimensiones de las métricas de los equilibradores de carga de red

Para filtrar las métricas del balanceador de carga, 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 balanceador de carga del modo siguiente: net/nombre-balanceador-carga/1234567890123456 (la última parte del ARN del balanceador de carga).
`TargetGroup`	Filtra los datos de métricas por grupo de destino. Especifique el grupo de destino del modo siguiente: targetgroup/nombre-grupo-destino/1234567890123456 (la última parte del ARN del grupo de destino).

Estadísticas correspondientes a las métricas del equilibrador de carga de red

CloudWatch proporciona estadísticas a partir de los puntos de datos de las métricas publicadas por Elastic Load Balancing. Las estadísticas son agregaciones de los datos de las métricas correspondientes al periodo especificado. Cuando se solicitan estadísticas, el flujo de datos devuelto se identifica mediante el nombre de la métrica y su dimensión. Una dimensión es un par de nombre/valor que identifica una métrica de forma inequívoca. Por ejemplo, puede solicitar estadísticas para todas las instancias EC2 en buen estado que se encuentran tras un 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. Los incrementos del valor máximo de `HealthyHostCount` se corresponden con las reducciones del valor mínimo de `UnHealthyHostCount`. Se recomienda monitorizar el valor máximo de `HealthyHostCount` e invocar la alarma cuando el valor máximo de `HealthyHostCount` caiga por debajo del mínimo requerido, o sea `0`. Esto puede ayudar a identificar cuándo sus destinos ya no están en buen estado. También se recomienda monitorizar el valor mínimo de `UnHealthyHostCount` e invocar la alarma cuando el valor mínimo de `UnHealthyHostCount` supere el valor de `0`. Esto permite detectar cuándo ya no hay ningún destino registrado.

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.

Visualización de las métricas de CloudWatch en el equilibrador de carga

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

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

Para consultar las métricas con la consola

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 elija 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 balanceador de carga y elija Monitoring.
   c. (Opcional) Para filtrar los resultados por tiempo, seleccione un intervalo de tiempo en Showing data for.
   d. Para obtener una vista más amplia de una misma métrica, seleccione su gráfico.

Para consultar métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres NetworkELB.
4. (Opcional) Para ver una métrica en todas las dimensiones, escriba su nombre en el campo de búsqueda.

Cómo ver métricas a través de la AWS CLI

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

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

Para obtener las estadísticas de una métrica desde la AWS CLI

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

```
aws cloudwatch get-metric-statistics --namespace AWS/NetworkELB \
--metric-name UnHealthyHostCount --statistics Average  --period 3600 \
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

A continuación, se muestra un ejemplo de la salida:

```
{
    "Datapoints": [
        {
            "Timestamp": "2017-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2017-04-18T04:00:00Z",
```

```
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Registros de acceso para el equilibrador de carga de red

Elastic Load Balancing proporciona registros de acceso que capturan información detallada sobre las conexiones TLS establecidas con el equilibrador de carga de red. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

Important

Aunque los registros de acceso tradicionales heredados (descritos en esta sección) permanecen disponibles, el equilibrador de carga de red ahora ofrece opciones de registro mejoradas mediante Registros de Amazon CloudWatch. Registros de Amazon CloudWatch ofrecen opciones de entrega más flexibles, incluida la entrega a Registros de Amazon CloudWatch, Amazon Data Firehose y Amazon Simple Storage Service. Para configurar estas opciones de registro mejoradas, visite la pestaña Integraciones del equilibrador de carga. Para obtener más información sobre Registros de Amazon CloudWatch, consulte Registros de CloudWatch para el equilibrador de carga de red.

Important

Los registros de acceso se crean solo si el equilibrador de carga tiene un oyente TLS y si los registros contienen información acerca de las solicitudes de TLS únicamente. Los registros de acceso registran las solicitudes en la medida de lo posible. Recomendamos utilizar los registros de acceso para comprender la naturaleza de las solicitudes y no como una relación exhaustiva de todas las solicitudes.

El registro de acceso es una característica opcional de Elastic Load Balancing que está desactivada de forma predeterminada. Una vez que se ha habilitado el registro de acceso del equilibrador de carga, Elastic Load Balancing captura los registros como archivos comprimidos y los almacena en el

bucket de Amazon S3 que haya especificado. Puede deshabilitar el registro de acceso en cualquier momento.

Puede habilitar el cifrado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) o con el servicio de administración de claves con claves administradas por el cliente (SSE-KMS CMK) para su bucket de S3. Cada archivo de registro de acceso se cifra automáticamente antes de que se almacene en su bucket de S3 y se descifra al acceder al mismo. No es necesario que haga nada, ya que no hay diferencia en la forma de acceder a los archivos de registro cifrados o sin cifrar. Cada archivo de registro se cifra con una clave única, que a su vez se cifra con una clave de KMS que se rota periódicamente. Para obtener más información, consulte Especificación del cifrado de Amazon S3 (SSE-S3) y Especificación del cifrado del servidor con AWS KMS (SSE-KMS) en la Guía del usuario de Amazon S3.

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

Contenido

Archivos de registro de acceso

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

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

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_net.load-balancer-id_end-time_random-string.log.gz
```

Bucket de

Nombre del bucket de S3.

prefijo

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

aws-account-id

El ID de la Cuenta de AWS del propietario.

region

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

aaaa/mm/dd

La fecha de entrega del registro.

load-balancer-id

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

end-time

La fecha y hora en que finalizó el intervalo de registro. Por ejemplo, la hora de finalización 20181220T2340Z contiene las entradas correspondientes a las solicitudes realizadas entre las 23:35 y las 23:40.

random-string

Una cadena generada aleatoriamente por el sistema.

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

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-
loadbalancer.1234567890abcdef_20200501T0000Z_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 almacenamiento en la Guía del usuario de Amazon S3.

Entradas de los registros de acceso

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. Al procesar los archivos de registro, debe hacer caso omiso de todos los campos no esperados situados al final de la entrada de registro.

Campo	Descripción
tipo	Tipo de agente de escucha. El valor admitido es `tls`.
versión	Versión de la entrada de registro. La versión actual es 2.0.
hora	El tiempo registrado al final de la conexión TLS en formato ISO 8601.
elb	ID de recurso del balanceador de carga.
agente de escucha	ID de recurso del agente de escucha TLS para la conexión.
client_port	Dirección IP y puerto del cliente.
destination_port	La dirección IP y el puerto de destino. Si el cliente se conecta directame nte al balanceador de carga, el destino es el agente de escucha. Si el cliente se conecta mediante un servicio de punto de enlace de VPC, el destino es el punto de enlace de VPC.
connection_time	Tiempo total para que se complete la conexión, desde el inicio al cierre, en milisegundos.
tls_handshake_time	Tiempo total para que se complete el protocolo de enlace TLS una vez establecida la conexión TCP, incluidos los retrasos del cliente, en milisegundos. Este tiempo se incluye en el campo `connection_time` . Si no hay un establecimiento de comunicación TLS o si el estableci miento de comunicación TLS falla, este valor se establece en `-`.
received_bytes	Número de bytes recibidos por el balanceador de carga desde el cliente después del descifrado.

Campo	Descripción
sent_bytes	Número de bytes enviados por el balanceador de carga al cliente antes del cifrado.
incoming_tls_alert	Valor entero de las alertas TLS recibidas por el balanceador de carga desde el cliente si lo hay. De lo contrario, este valor se establece en `-`.
chosen_cert_arn	ARN del certificado suministrado al cliente. Si no se envía un mensaje de saludo de cliente válido, este valor se establece en `-`.
chosen_cert_serial	Reservado para uso futuro. Este valor siempre se establece en `-`.
tls_cipher	Conjunto de cifrado negociado con el cliente en formato de OpenSSL. Si la negociación de TLS no se completa, este valor se establece en `-`.
tls_protocol_version	Protocolo TLS negociado con el cliente en formato de cadena. Los valores posibles son `tlsv10`, `tlsv11`, `tlsv12` y `tlsv13`. Si la negociación de TLS no se completa, este valor se establece en `-`.
tls_named_group	Reservado para uso futuro. Este valor siempre se establece en `-`.
domain_name	El valor de la extensión nombre_servidor del mensaje de saludo del cliente. Este valor está codificado como URL. Si no se ha enviado un mensaje de saludo de cliente válido o la extensión no está presente, el valor se establece en `-`.
alpn_fe_protocol	El protocolo de aplicación negociado con el cliente en formato de cadena. Los valores posibles son h2, `http/1.1` y `http/1.0`. Si no se configura ninguna política de ALPN en el agente de escucha TLS, no se encuentra ningún protocolo coincidente o no se envía ninguna lista de protocolos válida, este valor se establece en `-`.
alpn_be_protocol	El protocolo de aplicación negociado con el destino en formato de cadena. Los valores posibles son h2, `http/1.1` y `http/1.0`. Si no se configura ninguna política de ALPN en el agente de escucha TLS, no se encuentra ningún protocolo coincidente o no se envía ninguna lista de protocolos válida, este valor se establece en `-`.

Campo	Descripción
alpn_client_preference_list	El valor de la extensión application_layer_protocol_negotiation en el mensaje de saludo del cliente. Este valor está codificado como URL. Cada protocolo está entre comillas dobles y los protocolos están separados por comas. Si no se configura ninguna política de ALPN en el agente de escucha TLS, no se envía ningún mensaje de saludo de cliente válido o la extensión no está presente, este valor se establece en `-`. La cadena se trunca si tiene más de 256 bytes.
tls_connection_creation_time	El tiempo registrado al inicio de la conexión TLS en formato ISO 8601.

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.

A continuación se muestra un ejemplo para un agente de escucha TLS sin una política de ALPN.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - - 2018-12-20T02:59:30
```

A continuación se muestra un ejemplo para un agente de escucha TLS con una política de ALPN.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1" 2020-04-01T08:51:20
```

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 semejante cantidad de datos con el procesamiento línea por línea. En tal caso, podría ser preciso utilizar herramientas de análisis que ofrezcan soluciones de procesamiento en paralelo. Por ejemplo, puede utilizar las siguientes herramientas de análisis para analizar y procesar los 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 red en la Guía del usuario de Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

Habilitación de los registros de acceso del equilibrador de carga de red

Al habilitar el registro de acceso del balanceador de carga, debe especificar el nombre del bucket de S3 donde el balanceador de carga almacenará los logs. El bucket debe tener una política de bucket que conceda permiso a Elastic Load Balancing para escribir en el bucket.

> **Important**
>
> Los registros de acceso se crean solo si el equilibrador de carga tiene un oyente TLS y si los registros contienen información acerca de las solicitudes de TLS únicamente.

Requisitos del bucket

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.
- El prefijo que especifique no debe incluir `AWSLogs`. Agregamos la parte del nombre de archivo que comienza por `AWSLogs` después del nombre del bucket y el prefijo que especifique.
- El bucket debe tener una política que conceda permiso 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.

Ejemplo de política de bucket

A continuación, se muestra una política de ejemplo. Para los elementos `Resource`, sustituya *`amzn-s3-demo-destination-bucket`* con el nombre del bucket de S3 para los registros de acceso. Asegúrese de omitir *`Prefix/`* si no utiliza un prefijo de bucket. Para `aws:SourceAccount`, especifique el ID de la cuenta de AWS con el equilibrador de carga. Para `aws:SourceArn`, sustituya *`region`* y *`012345678912`* con la región y el ID de cuenta del equilibrador de carga, respectivamente.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
```

```
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-
bucket/Prefix/AWSLogs/account-ID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        }
    ]
}
```

Cifrado

Puede habilitar el cifrado del lado del servidor para su bucket de registro de acceso a Amazon S3 de una de las siguientes maneras:

- Claves administradas de Amazon S3 (SSE-S3)
- Claves de AWS KMS almacenadas en AWS Key Management Service (SSE-KMS) †

† Con los registros de acceso del equilibrador de carga de red, no puede usar claves administradas por AWS, debe usar claves administradas por el cliente.

Para obtener más información, consulte Especificación del cifrado de Amazon S3 (SSE-S3) y Especificación del cifrado del servidor con AWS KMS (SSE-KMS) en la Guía del usuario de Amazon S3.

La política de claves debe permitir al servicio cifrar y descifrar los registros. A continuación, se muestra una política de ejemplo.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

Configuración de los registros de acceso

Utilice el siguiente procedimiento para configurar los registros de acceso para capturar información de solicitudes y entregar los archivos de registro al bucket de S3.

Console

Para habilitar los registros de acceso

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://*amzn-s3-demo-logging-bucket*/*logging-prefix*
   - URI sin prefijo: s3://*amzn-s3-demo-logging-bucket*
7. Seleccione Save changes (Guardar cambios).

AWS CLI

Para habilitar los registros de acceso

Use el comando modify-load-balancer-attributes con los atributos relacionados.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes \
        Key=access_logs.s3.enabled,Value=true \
        Key=access_logs.s3.bucket,Value=amzn-s3-demo-logging-bucket \
        Key=access_logs.s3.prefix,Value=logging-prefix
```

CloudFormation

Para habilitar los registros de acceso

Actualice el recurso AWS::ElasticLoadBalancingV2::LoadBalancer para incluir los atributos relacionados.

```
Resources:
  myLoadBalancer:
```

```
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "access_logs.s3.enabled"
          Value: "true"
        - Key: "access_logs.s3.bucket"
          Value: "amzn-s3-demo-logging-bucket"
        - Key: "access_logs.s3.prefix"
          Value: "logging-prefix"
```

Deshabilitación de los registros de acceso del equilibrador de carga de red

Puedes deshabilitar el registro de acceso del balanceador de carga en cualquier momento. Después de deshabilitar el registro de acceso, los logs de acceso permanecerán en el bucket de S3 hasta que los elimine. Para obtener más información, consulte Creación, configuración y uso de buckets de S3 en la Guía del usuario de Amazon S3.

Console

Para desactivar los registros de acceso

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. Seleccione Save changes (Guardar cambios).

AWS CLI

Para desactivar los registros de acceso

Utilice el comando modify-load-balancer-attributes.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes Key=access_logs.s3.enabled,Value=false
```

Solución de problemas del equilibrador de carga de red

La siguiente información puede ayudarlo a solucionar problemas del equilibrador de carga de red.

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 grupos de destino del equilibrador de carga de red.

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

Los grupos de seguridad asociados a una instancia deben permitir el tráfico del balanceador de carga a través del puerto y el protocolo de comprobación de estado. Para obtener más información, consulte Grupos de seguridad de destino. Además, el grupo de seguridad del equilibrador de carga debe permitir el tráfico dirigido a las instancias. Para obtener más información, consulte Actualización de los grupos de seguridad del equilibrador de carga de red.

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

La ACL de red asociada a las subredes de sus instancias y a las subredes del equilibrador de carga debe permitir que el equilibrador de carga realice comprobaciones de estado y tráfico. Para obtener más información, consulte ACL de red.

Las solicitudes no se direccionan a los destinos.

Compruebe lo siguiente:

Hay un grupo de seguridad que no permite el tráfico

Los grupos de seguridad asociados a las instancias deben permitir el tráfico procedente de las direcciones IP (si los destinos se especifican mediante el ID de instancia) o de los nodos del balanceador de carga (si los destinos se especifican mediante una dirección IP) en el puerto de escucha. Para obtener más información, consulte Grupos de seguridad de destino. Además, el

grupo de seguridad del equilibrador de carga debe permitir el tráfico dirigido a las instancias. Para obtener más información, consulte Actualización de los grupos de seguridad del equilibrador de carga de red.

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

Las ACL de red asociadas con las subredes de la VPC deben permitir que el balanceador de carga y los destinos se comuniquen en ambas direcciones en el puerto de escucha. Para obtener más información, consulte ACL de red.

Los destinos se encuentran en una zona de disponibilidad que no está habilitada

Si registra los destinos en una zona de disponibilidad pero no la habilita, estos destinos registrados no recibirán tráfico del balanceador de carga.

La instancia está en una VPC interconectada

Si tiene instancias en una VPC interconectada con la VPC del balanceador de carga, debe registrarlas en el balanceador de carga por dirección IP, no por ID de instancia.

El ID de servidor configurado no coincide con el ID configurado en el destino

Si utiliza oyentes QUIC, asegúrese de que el ID configurado en el destino coincida con el ID configurado en el grupo de destino del equilibrador de carga de red.

Los destinos reciben más solicitudes de comprobación de estado de las que se esperaban

Las comprobaciones de estado de un equilibrador de carga de red se distribuyen y utilizan un mecanismo de consenso para determinar el estado del destino. Por tanto, los destinos reciben un número mayor de comprobaciones de estado que el que se estableció en el ajuste `HealthCheckIntervalSeconds`.

Los destinos reciben menos solicitudes de comprobación de estado de las que se esperaban

Compruebe si `net.ipv4.tcp_tw_recycle` está habilitado. Se sabe que este ajuste causa problemas con los balanceadores de carga. El ajuste `net.ipv4.tcp_tw_reuse` se considera una alternativa más segura.

Destinos en mal estado reciben solicitudes del balanceador de carga

Esto ocurre cuando todos los destinos registrados están en mal estado. Si hay al menos un destino registrado en buen estado, el equilibrador de carga de red solamente enrutará las solicitudes a los destinos registrados en buen estado.

Cuando todos los destinos registrados están en mal estado, el equilibrador de carga de red enruta las solicitudes a todos los destinos registrados, lo que se conoce como modo de apertura por error. El equilibrador de carga de red hace esto en lugar de eliminar todas las direcciones IP del DNS cuando todos los destinos están en mal estado y las zonas de disponibilidad respectivas no tienen un destino en buen estado al que enviar la solicitud.

El destino falla en las comprobaciones de estado HTTP o HTTPS debido a la falta de coincidencia del encabezado de host

El encabezado de host HTTP en la solicitud de comprobación de estado contiene la dirección IP del nodo del balanceador de carga y el puerto del agente de escucha, no la dirección IP del destino y el puerto de comprobación de estado. Si está asignando solicitudes entrantes por encabezado de host, debe asegurarse de que las comprobaciones de estado coincidan con cualquier encabezado de host HTTP. Otra opción es agregar un servicio HTTP independiente en un puerto diferente y configurar el grupo de destino para que utilice ese puerto para comprobaciones de estado en su lugar. Alternativamente, plantéese el uso de comprobaciones de estado TCP.

No se puede asociar un grupo de seguridad a un equilibrador de carga

Si el equilibrador de carga de red se creó sin grupos de seguridad, no podrá admitir grupos de seguridad después de su creación. Solo puede asociar un grupo de seguridad a un equilibrador de carga durante la creación, o a equilibrador de carga existente que se creó originalmente con grupos de seguridad.

No se pueden eliminar todos los grupos de seguridad

Si el equilibrador de carga de red se creó con grupos de seguridad, debe haber al menos un grupo de seguridad asociado a él en todo momento. No pueden eliminar todos los grupos de seguridad del equilibrador de carga al mismo tiempo.

Aumento de la métrica TCP_ELB_Reset_Count

Para cada solicitud de TCP que un cliente realiza a través de un equilibrador de carga de red, se controla el estado de la conexión. Si transcurre el tiempo de inactividad sin que el cliente ni el destino envíen datos a través de la conexión, esta se cierra. Si un cliente o un destino envía datos una vez transcurrido el tiempo de inactividad, recibirá un paquete TCP RST que indicará que la conexión ya no es válida. Además, si un destino no está en buen estado, el equilibrador de carga envía un RST TCP para los paquetes recibidos en las conexiones de cliente asociadas al destino, a menos que el destino en mal estado active el modo de apertura por error en el equilibrador de carga.

Si observa un aumento en la métrica `TCP_ELB_Reset_Count` justo antes o justo a medida que la métrica `UnhealthyHostCount` aumenta, es probable que los paquetes RST de TCP se hayan enviado porque el destino estaba empezando a fallar, pero no se había marcado como en mal estado. Si observa aumentos persistentes en `TCP_ELB_Reset_Count` sin que los destinos estén marcados como en mal estado, puede comprobar los registros de flujo de la VPC para ver si hay clientes que envíen datos sobre flujos caducados.

Se agota el tiempo de espera de conexión para las solicitudes enviadas desde un destino a su balanceador de carga

Compruebe si la preservación de la IP del cliente está habilitada en su grupo de destino. El bucle invertido de NAT, también conocido como horquilla, no se admite cuando la preservación de la IP del cliente está habilitada.

Si una instancia es cliente de un equilibrador de carga en el que está registrada y tiene habilitada la conservación de la IP del cliente, la conexión solo se completa si la solicitud se enruta a otra instancia diferente. Si la solicitud se enruta a la misma instancia desde la que se envió, se agota el tiempo de espera de la conexión porque las direcciones IP de origen y destino son las mismas. Tenga en cuenta que esto se aplica a pods de Amazon EKS que se ejecutan en la misma instancia de nodo de trabajo de EC2, incluso si tienen direcciones IP distintas.

Si una instancia debe enviar solicitudes a un balanceador de carga con el que está registrada, realice una de las siguientes operaciones:

- Preservación de la IP del cliente En su lugar, utilice el protocolo proxy, versión 2 para obtener la dirección IP del cliente.
- Asegúrese de que los contenedores que deben comunicarse se encuentran en diferentes instancias de contenedor.

El rendimiento se reduce cuando se trasladan destinos a un equilibrador de carga de red.

Tanto los equilibradores de carga clásicos como los equilibradores de carga de conexión utilizan la multiplexación de conexiones, pero los equilibradores de carga de red no. Por tanto, los destinos puede recibir más conexiones TCP detrás de un equilibrador de carga de red. Asegúrese de que los destinos estén listos para administrar el volumen de solicitudes de conexión que reciben.

Errores de asignación de puertos para flujos de backend

Con tráfico de PrivateLink o cuando la conservación de la IP del cliente está desactivada, un equilibrador de carga de red admite hasta 55 000 conexiones simultáneas o aproximadamente 55 000 conexiones por minuto para cada destino único (dirección IP y puerto). Si se superan estos límites, aumenta la probabilidad de errores de asignación de puertos. Puede realizar el seguimiento de los errores de asignación de puertos mediante la métrica `PortAllocationErrorCount`. Puede realizar el seguimiento de las conexiones activas mediante la métrica `ActiveFlowCount`. Para obtener más información, consulte Métricas de CloudWatch para el equilibrador de carga de red.

Para corregir los errores de asignación de puertos, recomendamos agregar destinos al grupo de destino.

Como alternativa, si no puede agregar destinos al grupo de destino, puede agregar hasta 7 direcciones IP secundarias a las interfaces de red del equilibrador de carga. Las direcciones IP secundarias se asignan automáticamente a partir de los bloques de CIDR IPv4 de las subredes correspondientes. Cada dirección IP secundaria consume 6 unidades de direccionamiento de red. Tenga en cuenta que, una vez que agrega una dirección IP secundaria, no puede eliminarla. La única forma de liberar las direcciones IP secundarias es eliminar el equilibrador de carga.

Fallos intermitentes en el establecimiento de conexiones TCP o retrasos en establecimiento de conexiones TCP

Cuando la conservación de la dirección IP del cliente está habilitada, un cliente se puede conectar a direcciones IP de destino distintas mediante el mismo puerto efímero de origen. Estas direcciones IP de destino pueden pertenecer al mismo equilibrador de carga (en zonas de disponibilidad diferentes) cuando el equilibrio de carga entre zonas está habilitado o a equilibradores de carga de red distintos que utilizan la misma dirección IP y puerto de destino registrados. En este caso, si estas conexiones se enrutan hacia la misma dirección IP y puerto de destino, el destino percibe una conexión duplicada, ya que ambas conexiones provienen de la misma dirección IP y puerto del cliente. Esto provoca errores y retrasos de conexión al establecer una de estas conexiones. Esta situación ocurre con frecuencia cuando existe un dispositivo NAT delante del cliente y se asignan la misma dirección IP y el mismo puerto de origen al conectarse simultáneamente a varias direcciones IP de equilibradores de carga de red.

Para reducir este tipo de error de conexión, puede aumentar el número de puertos efímeros de origen asignados por el cliente o el dispositivo NAT, o incrementar el número de destinos del equilibrador de carga. Recomendamos que los clientes cambien el puerto de origen que utilizan al reintentar la conexión después de estos fallos de conexión. Para evitar este tipo de error de conexión, si utiliza un único equilibrador de carga de red, puede considerar desactivar el equilibrio de carga entre zonas; si utiliza varios equilibradores de carga de red, puede considerar no usar la misma dirección IP y puerto de destino registrados en varios grupos de destino. Como alternativa, puede considerar desactivar la conservación de la IP del cliente. Si necesita la dirección IP del cliente, puede obtenerla mediante el protocolo proxy, versión 2. Para obtener más información sobre el protocolo proxy, versión 2, consulte Protocolo de proxy.

Posible error al aprovisionar el equilibrador de carga

Una de las razones por las que un equilibrador de carga de red puede fallar durante el aprovisionamiento es si utiliza una dirección IP que ya está asignada o que está asignada en otro lugar (por ejemplo, asignada como dirección IP secundaria para una instancia de EC2). Esta dirección IP impide que se configure el equilibrador de carga y su estado es `failed`. Para resolver este problema, desasigne la dirección IP asociada y vuelva a intentar el proceso de creación.

El tráfico se distribuye de forma desigual entre los destinos

Los oyentes TCP y TLS enrutan conexiones TCP, y los oyentes UDP enrutan flujos UDP. El equilibrador de carga selecciona los destinos mediante un algoritmo hash de flujo. Una conexión individual de un cliente es intrínsecamente persistente.

Si observa que algunos destinos parecen recibir más tráfico que otros, recomendamos revisar los registros de flujo de la VPC. Compare el número de conexiones únicas para cada dirección IP de destino. Mantenga el intervalo de tiempo lo más breve posible, ya que el registro, la anulación del registro y los destinos en mal estado influyen en estos recuentos de conexiones.

A continuación se indican escenarios posibles en los que las conexiones se pueden distribuir de forma desigual:

- Si comienza con un número reducido de destinos y luego registra destinos adicionales, los destinos originales aún mantienen conexiones con los clientes. Con una carga de trabajo HTTP, las conexiones persistentes garantizan que los clientes reutilicen las conexiones. Si reduce el valor máximo de conexiones persistentes en la aplicación web, los clientes abrirán nuevas conexiones con mayor frecuencia.
- Si la persistencia del grupo de destino está habilitada, existe un número reducido de clientes y estos se comunican a través de un dispositivo NAT con una única dirección IP de origen, las conexiones de estos clientes se enrutan al mismo destino.
- Si el equilibrio de carga entre zonas está desactivado y los clientes prefieren la dirección IP del equilibrador de carga de una de las zonas de disponibilidad, las conexiones se distribuyen de forma desigual entre las zonas del equilibrador de carga.

La resolución de nombres DNS contiene menos direcciones IP que las zonas de disponibilidad habilitadas

Lo ideal sería que su equilibrador de carga de red proporcionara una dirección IP por cada zona de disponibilidad habilitada, cuando tuviera al menos un host en buen estado en la zona de disponibilidad. Si no hay un host en buen estado en una zona de disponibilidad determinada y el equilibrio de carga entre zonas está deshabilitado, la dirección IP del equilibrador de carga de red correspondiente a esa zona de disponibilidad se eliminará del DNS.

Por ejemplo, supongamos que su equilibrador de carga de red tiene habilitadas tres zonas de disponibilidad y todas tienen al menos una instancia de destino registrada en buen estado.

- Si las instancias de destino registradas en la zona de disponibilidad A dejan de funcionar, la dirección IP correspondiente de la zona de disponibilidad A para el equilibrador de carga de red se elimina del DNS.
- Si dos de las zonas de disponibilidad habilitadas no tienen ninguna instancia de destino registrada en buen estado, las dos direcciones IP respectivas del equilibrador de carga de red se eliminarán del DNS.
- Si no hay ninguna instancia de destino registrada en buen estado en todas las zonas de disponibilidad habilitadas, se habilita el modo de apertura por error y, como resultado, el DNS proporcionará todas las direcciones IP de las tres zonas de disponibilidad habilitadas.

Los paquetes IP fragmentados no se enrutan a los destinos

Los equilibradores de carga de red no admiten paquetes IP fragmentados para tráfico que no sea UDP.

Solución de problemas de destinos en mal estado mediante el mapa de recursos

Si los destinos del equilibrador de carga de red no superan las comprobaciones de estado, puede utilizar el mapa de recursos para buscar destinos en mal estado y tomar medidas en función del código del motivo del error. Para obtener más información, consulte Visualización del mapa de recursos del equilibrador de carga de red.

El mapa de recursos ofrece dos vistas: Información general y Mapa de destinos en mal estado. La vista Información general está seleccionada de manera predeterminada y muestra todos los recursos del equilibrador de carga. Si selecciona la vista Mapa de destinos en mal estado, solo se mostrarán los destinos en mal estado de cada grupo de destino asociado al equilibrador de carga de red.

> **Note**
>
> La opción Mostrar detalles del recurso debe estar habilitada para ver el resumen de la comprobación de estado y los mensajes de error de todos los recursos aplicables del mapa de recursos. Si no está habilitada, debe seleccionar cada recurso para ver sus detalles.

La columna Grupos de destino muestra un resumen de los destinos en buen y mal estado de cada grupo de destino. Esto puede ayudar a determinar si ninguno de los destinos está superando las comprobaciones de estado, o si son solo destinos concretos los que no las superan. Si ninguno de los destinos de un grupo de destino supera las comprobaciones de estado, revise la configuración de comprobación de estado del grupo de destino. Seleccione el nombre de un grupo de destino para abrir su página de detalles en una pestaña nueva.

La columna Destinos muestra el ID de destino y el estado actual de la comprobación de estado de cada destino. Cuando un destino no está en buen estado, se muestra el código del motivo del error de la comprobación de estado. Cuando sea un único destino el que no supera una comprobación de estado, verifique que el destino tiene recursos suficientes. Seleccione el ID de un destino para abrir su página de detalles en una pestaña nueva.

Si selecciona Exportar, tiene la opción de exportar la vista actual del mapa de recursos del equilibrador de carga de red en formato PDF.

Verifique que la instancia no está superando las comprobaciones de estado y luego, en función del código del motivo del error, revise lo siguiente:

- Mal estado: tiempo de espera de la solicitud agotado
  - Compruebe que los grupos de seguridad y las listas de control de acceso (ACL) de la red asociados a los destinos y al equilibrador de carga de red no están bloqueando la conectividad.
  - Compruebe que el destino tenga suficiente capacidad disponible para aceptar conexiones desde el Equilibrador de carga de red.
  - Las respuestas a las comprobaciones de estado del equilibrador de carga de red se pueden ver en los registros de aplicaciones de cada destino. Para obtener más información, consulte Códigos de motivo de comprobación de estado.
- Mal estado: comprobaciones de estado no superadas
  - Compruebe que el destino esté escuchando el tráfico en el puerto de la comprobación de estado.

> **Cuando se utiliza un oyente TLS**
>
> Puede seleccionar qué política de seguridad se utiliza para las conexiones frontend. La política de seguridad utilizada para las conexiones backend se selecciona automáticamente en función de la política de seguridad frontend que se utilice.

- Si el oyente TLS utiliza una política de seguridad de TLS 1.3 para las conexiones frontend, se utiliza la política de seguridad `ELBSecurityPolicy-TLS13-1-0-2021-06` para las conexiones backend.
- Si el oyente TLS no utiliza una política de seguridad de TLS 1.3 para las conexiones frontend, se utiliza la política de seguridad `ELBSecurityPolicy-2016-08` para las conexiones backend.

Para obtener más información, consulte Políticas de seguridad.

- Compruebe que el destino proporciona un certificado de servidor y una clave con el formato correcto especificado en la política de seguridad.
- Compruebe que el destino admite uno o varios cifrados coincidentes y un protocolo proporcionado por el equilibrador de carga de red para establecer protocolos de enlace TLS.

Cuotas para los equilibradores de carga de red

Su Cuenta de AWS tiene cuotas predeterminadas, anteriormente conocidas como “límites”, para cada servicio de AWS. A menos que se indique otra cosa, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

A fin de ver las cuotas para los equilibradores de carga de red, abra la Consola de Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione Elastic Load Balancing. También puede utilizar 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, envíe una solicitud para aumentar la cuota del servicio.

Cuotas

- Balanceador de carga
- Grupos de destino
- Unidades de capacidad del equilibrador de carga

Balanceador de carga

Su Cuenta de AWS incluye las siguientes cuotas en relación con los equilibradores de carga de red.

Nombre	Valor predeterminado	Ajustable
Certificados por equilibrador de carga de red	25	Sí
Oyentes por equilibrador de carga de red	50	No
ENI del equilibrador de carga de red por VPC	1200 [1]	Sí
Balanceadores de carga de red por región	50	Sí
Destinos por zona de disponibilidad por equilibrador de carga de red	500 [2, 3]	Sí

Nombre	Valor predeterminado	Ajustable
Destinos por equilibrador de carga de red	3000 [3]	Sí

[1] Cada equilibrador de carga de red utiliza una interfaz de red por zona. La cuota se establece en el nivel de VPC. Al compartir subredes o VPC, el uso se calcula entre todos los inquilinos.

[2] Si un destino se encuentra registrado con N grupos de destino, cuenta como N destinos para este límite. Cada equilibrador de carga de aplicación que sea un destino del equilibrador de carga de red cuenta como 50 destinos si el equilibrio de carga entre zonas se encuentra deshabilitado o 100 destinos si el equilibrio de carga entre zonas se encuentra habilitado.

[3] Si el equilibrio de carga entre zonas se encuentra habilitado, el máximo es de 500 destinos por equilibrador de carga, independientemente del número de zonas de disponibilidad.

Grupos de destino

Las cuotas siguientes son para grupos de destino.

Nombre	Valor predeterminado	Ajustable
Grupos de destino por región	3000 [1]	Sí
Destinos por grupo de destino por región (instancias o direcciones IP)	1 000	Sí
Destinos por grupo de destino por región (equilibradores de carga de aplicación)	1	No

[1] Esta cuota se comparte entre los equilibradores de carga de aplicación y los equilibradores de carga de red.

Unidades de capacidad del equilibrador de carga

Las siguientes cuotas se aplican a las unidades de capacidad del equilibrador de carga (LCU).

Nombre	Valor predeterminado	Ajustable
Unidades de capacidad del equilibrador de carga de red (LCU) reservadas por equilibrador de carga de red y por zona de disponibilidad	45000	Sí
Unidades de capacidad de equilibradores de carga de red (LCU) reservadas por región	0	Sí

Historial de documentos para equilibradores de carga de red

En la tabla siguiente, se describen las versiones de los equilibradores de carga de red.

Cambio	Descripción	Fecha
Grupos de destino ponderados	Esta versión agrega compatibilidad con la acción predeterminada con grupos de destino ponderados.	19 de noviembre de 2025
Compatibilidad con los protocolos QUIC y TCP_QUIC	Esta versión agrega compatibilidad con los protocolos QUIC y TCP_QUIC.	13 de noviembre de 2025
Direcciones IPv4 secundarias	Esta versión agrega compatibilidad para agregar direcciones IPv4 secundarias a las interfaces de red del equilibrador de carga.	29 de julio de 2025
Desactivación de zonas de disponibilidad	Esta versión agrega compatibilidad para desactivar una zona de disponibilidad en un equilibrador de carga existente.	13 de febrero de 2025
Reserva de unidades de capacidad	Esta versión agrega compatibilidad para establecer una capacidad mínima para el equilibrador de carga.	20 de noviembre de 2024
Compatibilidad con UDP sobre IPv6 para equilibradores de carga de doble pila	Esta versión permite que los clientes accedan a aplicaciones basadas en UDP mediante IPv6.	31 de octubre de 2024

Certificados RSA de 3072 bits y ECDSA de 256/384/521 bits	Esta versión agrega compatibilidad con certificados RSA de 3072 bits y certificados de algoritmo de firma digital de curva elíptica (ECDSA) de 256, 384 y 521 bits mediante AWS Certificate Manager (ACM).	19 de enero de 2024
Finalización de TLS con FIPS	Esta versión agrega políticas de seguridad que utilizan módulos criptográficos FIPS 140-3 cuando se finalizan conexiones TLS.	20 de noviembre de 2023
Afinidad de DNS de zona	Esta versión agrega compatibilidad con clientes que resuelven el DNS del equilibrador de carga para recibir una dirección IP en la misma zona de disponibilidad (AZ) en la que se encuentran.	12 de octubre de 2023
Deshabilitación de la finalización de conexiones de destinos en mal estado	Esta versión agrega compatibilidad para mantener conexiones activas con destinos que no superen comprobaciones de estado.	12 de octubre de 2023
Finalización de conexiones UDP predeterminada	Esta versión agrega compatibilidad para finalizar conexiones UDP cuando concluye el tiempo de espera de anulación del registro de manera predeterminada.	12 de octubre de 2023

Registro de destinos mediante IPv6	Esta versión agrega compatibilidad para registrar instancias como destinos cuando se direccionan mediante IPv6.	2 de octubre de 2023
Grupos de seguridad para el equilibrador de carga de red	Esta versión permite asociar grupos de seguridad a los equilibradores de carga de red en el momento de su creación.	10 de agosto de 2023
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.	17 de noviembre de 2022
Configuración de la comprobación de estado	Esta versión proporciona mejoras en la configuración de la comprobación de estado.	17 de noviembre de 2022
Equilibrio de carga entre zonas	Esta versión agrega compatibilidad para configurar el equilibrio de carga entre zonas en el nivel del grupo de destino.	17 de noviembre de 2022
Grupos de destino IPv	Esta versión agrega compatibilidad para configurar grupos de destino de IPv6 para equilibradores de carga de red.	23 de noviembre de 2021

Equilibradores de carga internos IPv	Esta versión agrega compatibilidad para configurar grupos de destino de IPv6 para equilibradores de carga de red.	23 de noviembre de 2021
TLS 1.3	Esta versión incorpora políticas de seguridad compatibles con la versión 1.3 de TLS.	14 de octubre de 2021
Equilibradores de carga de aplicación como destinos	Esta versión permite configurar un equilibrador de carga de aplicación como destino de un equilibrador de carga de red.	27 de septiembre de 2021
Preservación de la IP del cliente	Esta versión permite configurar la preservación de la IP del cliente.	4 de febrero de 2021
Política de seguridad para FS compatible con la versión 1.2 de TLS 1.2	Esta versión incorpora una política de seguridad para Forward Secrecy (FS) compatible con la versión 1.2 de TLS.	24 de noviembre de 2020
Modo de pila doble	Esta versión incorpora compatibilidad con el modo de pila doble, que permite a los clientes conectarse al equilibrador de carga mediante direcciones IPv4 e IPv6.	13 de noviembre de 2020

Finalización de la conexión al anular el registro	Esta versión permite cerrar las conexiones con los destinos que se hayan dado de baja una vez transcurrido el tiempo de espera para anular el registro.	13 de noviembre de 2020
Políticas de ALPN	Esta versión agrega compatibilidad para las listas de preferencias de negociación de protocolo de capa de aplicación (ALPN).	27 de mayo de 2020
Sesiones persistentes	Esta versión agrega soporte para sesiones rápidas basadas en el protocolo y la dirección IP de origen.	28 de febrero de 2020
Subredes compartidas	Esta versión permite especificar subredes que le compartieron desde otra Cuenta de AWS.	26 de noviembre de 2019
Direcciones IP privadas	Esta versión le permite proporcionar una dirección IP privada desde el intervalo de direcciones IPv4 de la subred que especifique al habilitar una zona de disponibilidad para un balanceador de carga interno.	25 de noviembre de 2019
Agregar subredes	Esta versión añade la compatibilidad para habilitar zonas de disponibilidad adicionales después de crear el balanceador de carga.	25 de noviembre de 2019

Políticas de seguridad para FS	Esta versión agrega compatibilidad para tres políticas de seguridad de secreto hacia adelante predefinidas adicionales.	8 de octubre de 2019
Compatibilidad con SNI	Esta versión incorpora soporte para Indicación de nombre de servidor (SNI).	12 de septiembre de 2019
Protocolo UDP	Esta versión incorpora compatibilidad con el protocolo UDP.	24 de junio de 2019
Disponibilidad en una nueva región	Esta versión agrega compatibilidad con equilibradores de carga de red en la región Asia-Pacífico (Osaka).	12 de junio de 2019
Protocolo TLS	Esta versión incorpora compatibilidad con el protocolo TLS.	24 de enero de 2019
Equilibrio de carga entre zonas	Esta versión incorpora compatibilidad para habilitar el balance de carga entre zonas.	22 de febrero de 2018
Proxy Protocol	Esta versión incorpora compatibilidad para habilitar Proxy Protocol.	17 de noviembre de 2017
Direcciones IP como destinos	Esta versión añade soporte para registrar direcciones IP como destinos.	21 de septiembre de 2017

Tipo de equilibrador de carga nuevo	Esta versión de Elastic Load Balancing presenta los equilibradores de carga de red.	7 de septiembre de 2017