Equilibrador de carga de red

Elastic Load Balancing

Elastic Load Balancing: Equilibrador de carga de red

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 admite los protocolos TCP, UDP, TCP_UDP y TLS. Puede registrar un destino en varios grupos de destino. Puede configurar las comprobaciones de estado de cada grupo de destino. Las comprobaciones de estado se llevan a cabo en todos los destinos registrados en un grupo de destino especificado en la regla del oyente del equilibrador de carga.

Para obtener más información, consulte la siguiente documentación sobre :

- 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 atender millones de solicitudes por segundo. Una vez que el balanceador de carga ha recibido una solicitud de conexión, selecciona un destino en el grupo de destino para la regla predeterminada. Intenta abrir una conexión TCP con el destino seleccionado en el puerto especificado en la configuración del agente de escucha.

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 Zonas de disponibilidad.

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 time-to-live (TTL) y envía solicitudes a la dirección IP después de eliminarla del DNS, las solicitudes fallan.

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.

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.
- Support para monitorizar el estado de cada servicio de forma independiente, ya que los controles de estado se definen a nivel del grupo objetivo y muchas CloudWatch métricas de Amazon se informan a nivel del grupo objetivo. Si adjunta un grupo de destino a un grupo de escalado automático, podrá escalar cada servicio de forma dinámica en función de la demanda.

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

Cómo comenzar

Para crear un equilibrador de carga de red, pruebe con uno de los siguientes tutoriales:

- Introducción a los equilibradores de carga de red
- Tutorial: Crear un equilibrador de carga de red mediante la AWS CLI

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

Precios

Para obtener más información, consulte Precio del equilibrador de carga de red.

Introducción a los equilibradores de carga de red

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

Tareas

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

Antes de empezar

- Decida qué zonas de disponibilidad va a utilizar con las instancias EC2. Configure la nube privada virtual (VPC) con al menos una subred pública en cada una de estas zonas de disponibilidad. Estas subredes públicas se utilizan para configurar el equilibrador de carga. Puede lanzar las instancias EC2 en otras subredes de estas zonas de disponibilidad en su lugar.
- Lance al menos una instancia EC2 en cada zona de disponibilidad. Asegúrese de que los grupos de seguridad de estas instancias permiten el acceso mediante TCP de los clientes del puerto del agente de escucha y las solicitudes de comprobación de estado procedentes de la VPC. Para obtener más información, consulte Grupos de seguridad de destino.

Paso 1: configurar el grupo de destino

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

Para configurar su grupo objetivo mediante la consola

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

Paso 2: Elegir un tipo de equilibrador de carga

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

Para crear un Network Load Balancer mediante la consola

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

Paso 3: configurar el equilibrador de carga y el oyente

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

Para configurar el equilibrador de carga y el oyente

1. En Load Balancer name (Nombre del equilibrador de carga), escriba un nombre para el equilibrador de carga. Por ejemplo, `my-nlb`.
2. Para Scheme y IP address type, mantenga los valores predeterminados.
3. En Asignación de red, seleccione la VPC que ha utilizado para las instancias de EC2. En cada una de las zonas de disponibilidad que utilizó para lanzar las instancias EC2, seleccione la zona de disponibilidad y después seleccione una subred pública de esa zona de disponibilidad.

   De forma predeterminada, AWS asigna una dirección IPv4 a cada nodo del equilibrador de carga de la subred de su zona de disponibilidad. De forma alternativa, cuando crea un balanceador de carga expuesto a Internet, puede seleccionar una dirección IP elástica para cada zona de disponibilidad. Esto proporciona al balanceador de carga direcciones IP estáticas.
4. En Grupos de seguridad, preseleccionamos el grupo de seguridad predeterminado para su VPC. Puede seleccionar otros grupos de seguridad, según sea necesario. Si no cuenta con un grupo de seguridad adecuado, elija Crear un grupo de seguridad nuevo y cree uno que cumpla con sus necesidades de seguridad. Para obtener más información, consulte Crear un grupo de seguridad en la Guía del usuario de Amazon VPC.

   > **Warning**
   >
   > Si no asocia ahora un grupo de seguridad al equilibrador de carga, no podrá asociarlo más adelante.
5. En Oyentes y enrutamiento, mantenga el protocolo y el puerto predeterminados y seleccione el grupo de destino de la lista. Esto configura un oyente que acepta el tráfico de TCP en el puerto 80 y reenvía el tráfico al grupo de destino seleccionado de forma predeterminada.

6. (Opcional) Agregue etiquetas para categorizar su equilibrador de carga. Las claves de las etiquetas deben ser únicas en cada equilibrador de carga. Los caracteres permitidos son letras, espacios y números (en UTF-8), además de los siguientes caracteres especiales: + - =. _ : / @. No utilice espacios iniciales ni finales. Los valores distinguen entre mayúsculas y minúsculas.
7. Revise la configuración y elija Create load balancer (Crear equilibrador de carga). Durante la creación, se aplican algunos atributos predeterminados al equilibrador de carga. Puede verlos y editarlos después de crear el equilibrador de carga. Para obtener más información, consulte Atributos del equilibrador de carga.

Paso 4: Probar un equilibrador de carga

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

Para probar el equilibrador de carga

1. Una vez que se le notifique que el equilibrador de carga se ha creado correctamente, elija Close.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el grupo de destino que se acaba de crear.
4. Elija Targets y verifique que las instancias estén listas. Si el estado de una instancia es `initial`, puede deberse a que la instancia sigue en proceso de registro o no ha superado el número mínimo de comprobaciones de estado para que se considere correcta. Cuando el estado de al menos una instancia sea `healthy`, podrá probar el equilibrador de carga.
5. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
6. Seleccione el nombre del equilibrador de carga recién creado para abrir la página de detalles.
7. Copie el nombre DNS del balanceador de cargas (por ejemplo, -1234567890abcdef. elb.us-east-2.amazonaws.com). my-load-balancer 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.

Paso 5: (opcional) eliminar el equilibrador de carga

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

Tenga en cuenta que, cuando se elimina un equilibrador de carga, los destinos registrados con él no se ven afectados. Por ejemplo, las instancias EC2 seguirán en ejecución.

Para eliminar el balanceador de cargas mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibración de carga, elija equilibradores de carga.
3. Seleccione la casilla de verificación del equilibrador de carga y elija Acciones, Eliminar.
4. Cuando se le pida confirmación, ingrese **`confirm`** y elija Eliminar.

Tutorial: Crear un equilibrador de carga de red mediante la AWS CLI

En este tutorial, encontrará una introducción práctica sobre el uso de equilibradores de carga de red a través de la AWS CLI.

Antes de empezar

- Instale la AWS CLI o actualice a la versión actual de la AWS CLI si utiliza una versión que no admite equilibradores de carga de red. Para obtener más información, consulte Instalar la AWS Command Line Interface en la Guía del usuario de AWS Command Line Interface.
- Decida qué zonas de disponibilidad va a utilizar con las instancias EC2. Configure la nube privada virtual (VPC) con al menos una subred pública en cada una de estas zonas de disponibilidad.
- Decida si creará un equilibrador de carga de pila doble o IPv4. Utilice IPv4 si desea que los clientes se comuniquen con el equilibrador de carga solo mediante direcciones IPv4. Utilice la pila doble si desea que los clientes se comuniquen con el equilibrador de carga mediante direcciones IPv4 e IPv6. También puede utilizar la pila doble para comunicarse con destinos de backend, como aplicaciones IPv6 o subredes de pila doble, mediante IPv6.
- Lance al menos una instancia EC2 en cada zona de disponibilidad. Asegúrese de que los grupos de seguridad de estas instancias permiten el acceso mediante TCP de los clientes del puerto del agente de escucha y las solicitudes de comprobación de estado procedentes de la VPC. Para obtener más información, consulte Grupos de seguridad de destino.

Crear el equilibrador de carga IPv4

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

Para crear un equilibrador de carga IPv4

1. Usa el create-load-balancercomando para crear un balanceador de cargas IPv4, especificando una subred pública para cada zona de disponibilidad en la que lanzaste instancias. Puede especificar solo una subred por zona de disponibilidad.

   De forma predeterminada, cuando los equilibradores de carga de red se crean mediante la AWS CLI, no utilizan de forma automática el grupo de seguridad predeterminado para la VPC. Si no

asocia un grupo de seguridad al equilibrador de carga durante la creación, no podrá agregarlo más adelante. Recomendamos que especifique los grupos de seguridad para su equilibrador de carga durante la creación mediante la opción `--security-groups`.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --security-groups sg-0123456789EXAMPLE
```

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

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

2. Utilice el create-target-groupcomando para crear un grupo de destino IPv4, especificando la misma VPC que utilizó para las instancias de EC2. Los grupos de destino de IPv4 admiten destinos de tipo IP y de instancia.

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

El resultado contiene el ARN del grupo con este formato:

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

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

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

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

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

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

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

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

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

Crear el equilibrador de carga de pila doble

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

Para crear un equilibrador de carga de pila doble

1. Usa el create-load-balancercomando para crear un balanceador de cargas de doble pila, especificando una subred pública para cada zona de disponibilidad en la que hayas lanzado las instancias. Puede especificar solo una subred por zona de disponibilidad.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
 subnet-0e3f5cac72EXAMPLE --ip-address-type dualstack
```

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

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

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

   Debe utilizar un grupo destino de TCP o TLS con su equilibrador de carga de pila doble.

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

   Los grupos de destino IPv4 admiten destinos de tipo IP y de instancia. Los destinos IPv6 solo admiten destinos de IP.

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

El resultado contiene el ARN del grupo con este formato:

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

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

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

4. Utilice el comando create-oyente para crear un oyente del equilibrador de carga con una regla predeterminada que reenvíe las solicitudes al grupo de destino: Los equilibradores de carga de pila doble deben tener oyentes de TCP o TLS.

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

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

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

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

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

Especificar una dirección IP elástica para el balanceador de carga

Al crear un equilibrador de carga de red, puede especificar una dirección IP elástica para cada subred mediante una asignación de subred.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \
```

```
--subnet-mappings SubnetId=subnet-0e3f5cac72EXAMPLE,AllocationId=eipalloc-12345678
```

Eliminar el equilibrador de carga

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

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

Equilibrador de carga de red

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

Para configurar el equilibrador de carga, debe crear grupos de destino y, a continuación, registrar los destinos en esos grupos. El equilibrador de carga 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 balanceadores de carga de red admiten las conexiones de los clientes a través de interconexiones de VPC AWS AWS Direct Connect, VPN gestionada y soluciones de VPN de terceros.

Contenido

Estado del equilibrador de carga

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

`provisioning`

El equilibrador de carga se está configurando.

`active`

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

`failed`

El equilibrador de carga no se ha podido configurar.

Atributos del equilibrador de carga

Un equilibrador de carga cuenta con los siguientes atributos:

`access_logs.s3.enabled`

Indica si se encuentran 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, al evitar el acceso no intencionado a su equilibrador de carga interno a través de una puerta de enlace de Internet. Se ha establecido en `false` para los equilibradores de carga con acceso a Internet y

`true` para los equilibradores de carga internos. Este atributo no impide el acceso a Internet que no sea de IGW (por ejemplo, mediante peering, AWS Direct Connect Transit Gateway o). AWS VPN

`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 del equilibrador de carga. 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.

Tipo de dirección IP

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

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

`ipv4`

Los clientes deben conectarse al equilibrador de carga mediante direcciones IPv4 (por ejemplo, 192.0.2.1). Los equilibradores de carga compatibles con IPv4 (tanto internos como con acceso a Internet) admiten los oyentes de TCP, UDP, TCP_UDP y TLS.

`dualstack`

Los clientes pueden conectarse al equilibrador de carga mediante direcciones IPv4 (por ejemplo, 192.0.2.1) y direcciones IPv6 (por ejemplo, 2001:0db8:85a3:0:0:8a2e:0370:7334). Los equilibradores de carga compatibles con la pila doble (tanto internos como con acceso a Internet) admiten los oyentes de TCP y TLS.

Consideraciones

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

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

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

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

Mapa de recursos de Network Load Balancer

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

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

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

Componentes del mapa de recursos

Vistas de mapas

Hay dos vistas disponibles en el mapa de recursos de Network Load Balancer: Descripción general y Mapa objetivo poco saludable. La descripción general está seleccionada de forma predeterminada y muestra todos los recursos del balanceador de cargas. Al seleccionar la vista del mapa de objetivos en mal estado, solo se mostrarán los objetivos en mal estado y los recursos asociados a ellos.

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

Columnas de recursos

El mapa de recursos de Network Load Balancer contiene tres columnas de recursos, una para cada tipo de recurso. Los grupos de recursos son Listeners, Target groups y Targets.

Mosaicos de recursos

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

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

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

- Cada mosaico de recursos contiene un enlace que, cuando se selecciona, lleva a la página de detalles de ese recurso.
  - Listeners - Seleccione el protocolo de oyentes: puerto. Por ejemplo, `TCP:80`
  - Grupos objetivo - Seleccione el nombre del grupo objetivo. Por ejemplo, `my-target-group`
  - Objetivos - Seleccione el ID del objetivo. Por ejemplo, `i-1234567890abcdef0`

Exporte el mapa de recursos

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

Zonas de disponibilidad

Las zonas de disponibilidad del balanceador de carga se habilitan al crearlo. Si habilita varias zonas de disponibilidad para el balanceador de carga, esto aumenta la tolerancia a errores de las aplicaciones. No puede deshabilitar las zonas de disponibilidad para un equilibrador de carga de red tras su creación, pero puede habilitar zonas de disponibilidad adicionales.

Al habilitar una zona de disponibilidad, especifica una subred de dicha zona de disponibilidad. Elastic Load Balancing crea un nodo de equilibrador de carga en la zona de disponibilidad y una interfaz de red para la subred (la descripción empieza por “red de ELB” e incluye el nombre del equilibrador de carga). Cada nodo del balanceador de carga de la zona de disponibilidad utiliza esta interfaz de red para obtener una dirección IPv4. Tenga en cuenta que puede ver esta interfaz de red pero no puede modificarla.

Al crear un balanceador de carga expuesto a Internet, puede especificar una dirección IP elástica por cada subred. Si no elige una de sus direcciones IP elásticas, Elastic Load Balancing proporciona una dirección IP elástica por subred en su nombre. Estas direcciones IP elásticas proporcionan al balanceador de carga direcciones IP estáticas que no cambiarán durante la vida útil del balanceador de carga. No puede cambiar estas direcciones IP elásticas después de crear el equilibrador de carga.

Al crear un balanceador de carga interno, puede especificar una dirección IP privada por cada subred. Si no especifica una dirección IP de la subred, Elastic Load Balancing elige una en su nombre. Estas direcciones IP privadas proporcionan al balanceador de carga direcciones IP estáticas que no cambiarán durante la vida útil del balanceador de carga. No puede cambiar estas direcciones IP privadas después de crear el equilibrador de carga.

Consideraciones

- Para los balanceadores de carga expuestos a Internet, las subredes que especifique deben tener al menos 8 direcciones IP disponibles. En el caso de los balanceadores de carga internos, esto solo es necesario si permite AWS seleccionar una dirección IPv4 privada de la subred.
- No puede especificar una subred en una zona de disponibilidad restringida. El mensaje de error es "Los balanceadores de carga de tipo 'red' no son compatibles con nombre_zona_disponibilidad". Puede especificar una subred en otra zona de disponibilidad que no esté restringida y utilizar el balanceo de carga entre zonas para distribuir el tráfico en los destinos en la zona de disponibilidad restringida.
- Puede especificar subredes que se hayan compartido con usted.
- No se puede especificar una subred en una zona local.

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.

Para agregar zonas de disponibilidad a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Asignación de redes, seleccione Editar subredes.
5. Para habilitar una zona de disponibilidad, active su casilla de verificación. Si hay una subred en esa zona de disponibilidad, se seleccionará. Si hay más de una subred en esa zona de disponibilidad, seleccione una de ellas. Tenga en cuenta que puede seleccionar una sola subred por zona de disponibilidad.

   Para un balanceador de carga expuesto a Internet, puede seleccionar una dirección IP elástica para cada zona de disponibilidad. En el caso de un equilibrador de carga interno, puede asignar una dirección IP privada del rango IPv4 de cada subred en lugar de permitir que Elastic Load Balancing asigne una.
6. Elija Guardar cambios.

Para añadir zonas de disponibilidad mediante el AWS CLI

Utilice el comando set-subnets.

Equilibrio de carga entre zonas

De manera predetermina, cada nodo del balanceador de carga distribuye el tráfico entre los destinos registrados en su zona de disponibilidad solamente. Si activa el equilibrio de carga entre zonas, cada nodo del equilibrador de carga 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 “Equilibrio de carga entre zonas” y Equilibrio de carga entre zonas en la Guía del usuario de Elastic Load Balancing.

Protección contra eliminación

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

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

Para habilitar la protección contra eliminación desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione 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 Configuración, active Protección contra eliminación.
6. Elija Guardar cambios.

Para deshabilitar la protección contra eliminación desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione 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 Configuración, active Protección contra eliminación.
6. Elija Guardar cambios.

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

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

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 el cliente ni el

destinatario envíen datos a través de la conexión, esta se cierra. Si un cliente o destino envía datos una vez transcurrido el tiempo de inactividad, recibirá un paquete de RST de TCP que indicará que la conexión ya no es válida.

Establecemos el valor del tiempo de inactividad para los flujos de TCP en 350 segundos. No se puede modificar este valor. Los clientes o destinos pueden utilizar paquetes keepalive TCP para restablecer el tiempo de inactividad. Los paquetes keepalive que se han enviado para mantener las conexiones de TLS no pueden contener datos ni carga útil.

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.

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

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

En primer lugar, registre un nombre de dominio con un registrador de nombres de dominio acreditado. A continuación, utilice su servicio de DNS (por ejemplo, su registrador de dominio) para crear un registro de DNS y direccionar las consultas al equilibrador de carga. Para obtener más información, consulte la documentación de su servicio de DNS. Por ejemplo, si utiliza Amazon

Route 53 como servicio de DNS, crea un registro de alias que apunta a su equilibrador de carga. Para obtener más información, consulte Enrutamiento del tráfico a un equilibrador de carga de ELB en la Guía para desarrolladores de Amazon Route 53.

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

Linux o Mac

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

Windows

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

El balanceador de carga tiene registros DNS para sus nodos de balanceador de carga. Puede utilizar nombres de DNS con la siguiente sintaxis para determinar las direcciones IP de los nodos del equilibrador de carga: *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
```

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 de su equilibrador de carga de red recibirán cualquier dirección IP del equilibrador de carga en buen estado. Esto lleva a la distribución de las conexiones de los clientes entre las zonas de disponibilidad de los equilibradores de carga. 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 en 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.

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 preferirán la dirección IP del equilibrador de carga en su zona de disponibilidad. Las consultas se pueden resolver en otras zonas si no hay direcciones IP de equilibradores de carga en buen estado en su zona.
- Afinidad de zona de disponibilidad parcial: afinidad de zona del 85 por ciento

  El 85 por ciento de las consultas de DNS de los clientes prefieren las direcciones IP de los equilibradores de carga en su 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 de los equilibradores de carga en buen estado en todas las zonas de disponibilidad del equilibrador de carga.

> **Note**
>
> 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.

La afinidad de zona de disponibilidad ayuda a enrutar las solicitudes del cliente al equilibrador de carga, mientras que el equilibrio de carga entre zonas se utiliza para ayudar a enrutar las solicitudes desde el equilibrador de carga a los destinos. Cuando se utiliza la afinidad entre zonas de disponibilidad, se debe desactivar el equilibrio de carga entre zonas para garantizar que el tráfico del equilibrador de carga desde los clientes a los destinos permanezca dentro de la misma zona

de disponibilidad. Con esta configuración, el tráfico de los clientes se envía a la misma zona de disponibilidad de Network Load Balancer, por lo que se recomienda configurar la aplicación para que escale de forma independiente en cada zona de disponibilidad. Esta es una consideración importante cuando la cantidad de clientes por zona de disponibilidad y el tráfico por 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 de los equilibradores de carga 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.
- 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.

Supervisión

Se recomienda realizar un seguimiento de la distribución de las conexiones entre las zonas de disponibilidad mediante las métricas del equilibrador de carga de 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 CloudWatch métricas para su Network Load Balancer.

Activar la afinidad de zona de disponibilidad

En los pasos de este procedimiento se explica cómo activar la afinidad de zona de disponibilidad mediante la consola de Amazon EC2.

Para activar la afinidad de zona de disponibilidad mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.

5. 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. Elija Guardar cambios.

Para activar la afinidad entre zonas de disponibilidad mediante el AWS CLI

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

Desactivar la afinidad de zona de disponibilidad

En los pasos de este procedimiento se explica cómo desactivar la afinidad de zona de disponibilidad mediante la consola de Amazon EC2.

Para desactivar la afinidad de zona de disponibilidad mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En Configuración del enrutamiento de zonas de disponibilidad, Política de enrutamiento de clientes (registro de DNS), seleccione Cualquier zona de disponibilidad.
6. Elija Guardar cambios.

Para desactivar la afinidad entre zonas de disponibilidad mediante el AWS CLI

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

Crear un equilibrador de carga de red

Un balanceador de carga toma las solicitudes de los clientes y las distribuye entre los destinos de un grupo de destino; por ejemplo, instancias EC2.

Antes de empezar, asegúrese de que la nube privada virtual (VPC) para el balanceador de carga tiene al menos una subred pública en cada zona de disponibilidad en la que tiene destinos. También

debe configurar un grupo de destino y registrar al menos un destino para establecerlo como predeterminado a fin de enrutar el tráfico al grupo de destino.

Para crear un equilibrador de carga mediante el AWS CLI, consulteTutorial: Crear un equilibrador de carga de red mediante la AWS CLI.

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

Tareas

- Paso 1: Configurar un grupo de destino
- Paso 2: registrar destinos
- Paso 3: configurar un equilibrador de carga y un oyente
- Paso 4: probar el equilibrador de carga

Paso 1: Configurar un grupo de destino

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

Para configurar el grupo objetivo mediante la consola

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

    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.

d. (Opcional) En Port, modifique el valor predeterminado según sea necesario.

e. En Tipo de dirección IP, elija IPv4 o IPv6. Esta opción solo está disponible si el tipo de destino son instancias o direcciones IP y el protocolo es TCP o TLS.

   Debe asociar un grupo de destino de IPv6 a un equilibrador de carga de pila doble. Todos los destinos del grupo de destino deben tener el mismo tipo de dirección IP. No puede cambiar el tipo de dirección IP de un grupo de destino después de crearlo.

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 de la comprobación de estado avanzada, elija el puerto de comprobación de estado, el recuento, el tiempo de espera, el intervalo y los códigos de éxito. Si las comprobaciones de estado superan el recuento de UnhealthyThresholdCount, el equilibrador de carga inhabilita el destino. Cuando las comprobaciones de estado superan el recuento de HealthyThresholdCount, el equilibrador de carga vuelve a poner el destino en servicio. Para obtener más información, consulte Comprobaciones de estado de los grupos de destino.
6. (Opcional) Para agregar una etiqueta, expanda Etiquetas, elija Agregar etiqueta e ingrese una clave y un valor de etiqueta.
7. Elija Siguiente.

Paso 2: registrar destinos

Puede registrar instancias de EC2, direcciones IP o un equilibrador de carga de aplicación con su grupo de destino. Este es un paso opcional para crear un equilibrador de carga. Sin embargo, debe registrar sus destinos para asegurarse de que el equilibrador de carga pueda enrutar el tráfico hacia ellos.

1. En la página Registrar destinos, agregue uno o más destinos de la siguiente manera:
   - Si el tipo de destino es Instancias, seleccione las instancias, ingrese los puertos y, a continuación, elija Incluir como pendiente a continuación.
   - Si el tipo de destino es Direcciones IP, seleccione la red, ingrese las direcciones IP y los puertos y, a continuación, seleccione Incluir como pendiente a continuación.
   - Si el tipo de destino es Equilibrador de carga de aplicación, seleccione un equilibrador de carga de aplicación.

2. Elija Crear grupo de destino.

Paso 3: configurar un equilibrador de carga y un oyente

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

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

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

    a. En Load Balancer name (Nombre del equilibrador de carga), escriba un nombre para el equilibrador de carga. Por ejemplo, **`my-nlb`**. El nombre de su equilibrador de carga de red debe ser único dentro del conjunto de equilibradores de carga de aplicación y equilibradores de carga de red para 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 expuesto a Internet direcciona las solicitudes de los clientes a través de Internet hasta los destinos. Un equilibrador de carga interno direcciona las solicitudes hasta los destinos mediante direcciones IP privadas.

    c. En Tipo de dirección IP, elija IPv4 si sus clientes utilizan direcciones IPv4 para comunicarse con el equilibrador de carga o Pila doble si sus clientes utilizan tanto direcciones IPv4 como IPv6 a fin de comunicarse con el equilibrador de carga.

6. Asignación de redes

    a. En VPC, seleccione la VPC que ha utilizado para las instancias de EC2.

Si seleccionó Con acceso a Internet en Esquema, solo se pueden seleccionar las VPC con una puerta de enlace de Internet.

b. En Asignaciones, seleccione dos o más zonas de disponibilidad y las subredes correspondientes. Habilitar varias zonas de disponibilidad aumenta la tolerancia a errores de sus aplicaciones. Puede especificar subredes que se hayan compartido con usted.

   En el caso de los equilibradores de carga con acceso a Internet, puede seleccionar una dirección IP elástica para cada zona de disponibilidad. Esto proporciona al balanceador de carga direcciones IP estáticas. Como alternativa, en el caso de un balanceador de cargas interno, puedes asignar una dirección IP privada del rango IPv4 de cada subred en lugar de dejar que AWS te asignen una.

7. En Grupos de seguridad, preseleccionamos el grupo de seguridad predeterminado para su VPC. Puede seleccionar otros grupos de seguridad, según sea necesario. Si no cuenta con un grupo de seguridad adecuado, elija Crear un grupo de seguridad nuevo y cree uno que cumpla con sus necesidades de seguridad. Para obtener más información, consulte Crear un grupo de seguridad en la Guía del usuario de Amazon VPC.

   > ⚠ Warning
   >
   > Si no asocia ahora un grupo de seguridad al equilibrador de carga, no podrá asociarlo más adelante.

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 para redirigir el tráfico. Si anteriormente no creó un grupo de destino, debe crearlo ahora. También puede elegir Agregar oyente para agregar otro oyente (por ejemplo, un oyente de TLS).

   c. (Opcional) Agregue etiquetas para clasificar a su oyente.

   d. En Configuración de oyente seguro (disponible solo para los oyentes de TLS), realice lo siguiente:

      i. En Política de seguridad, elija una política de seguridad que cumpla con sus requisitos.

ii. Para la política de ALPN, elija una política para habilitar ALPN o elija None (Ninguna) para deshabilitar ALPN.

iii. En Certificado de SSL predeterminado, elija Desde ACM (recomendado) y seleccione un certificado. Si no dispone de un certificado disponible, puede importar un certificado a ACM o utilizar ACM para aprovisionar uno. Para obtener más información, consulte Emisión y administración de certificados en la Guía del usuario de AWS Certificate Manager .

9. (Opcional) Puedes usar servicios complementarios con tu balanceador de cargas. Por ejemplo, puedes elegir AWS Global Acceleratorcrear un acelerador para ti y asociar tu balanceador de cargas al acelerador. El nombre del acelerador puede tener los siguientes caracteres (hasta 64 caracteres): a-z, A-Z, 0-9,. (punto) y - (guión). Una vez creado el acelerador, vaya a la AWS Global Acceleratorconsola para terminar de configurarlo. Para obtener más información, consulte Añadir un acelerador al crear un balanceador de cargas
10. Etiquetas

    (Opcional) Agregue etiquetas para categorizar su equilibrador de carga. 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. Puede verlos y editarlos después de crear el equilibrador de carga. Para obtener más información, consulte Atributos del equilibrador de carga.

Paso 4: probar el equilibrador de carga

Después de crear el equilibrador de carga, puede comprobar 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, consulte Eliminar un equilibrador de carga de red.

Para probar el equilibrador de carga

1. Una vez creado el equilibrador de carga, elija Close (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 el estado de al menos una instancia sea healthy, podrá probar el equilibrador de carga. Para obtener más información, consulte Estado del destino.
5. En el panel de navegación, seleccione Equilibradores de carga.
6. Seleccione el equilibrador de carga nuevo.
7. Copia el nombre DNS del balanceador de cargas (por ejemplo, my-load-balancer -1234567890abcdef. elb.us-east-2.amazonaws.com). Pegue el nombre DNS en el campo de direcciones de un navegador web que esté conectado a Internet. Si todo funciona normalmente, el navegador mostrará la página predeterminada del servidor.

Tipos de direcciones IP para el equilibrador de carga de red

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

Requisitos de la pila doble

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

Para establecer el tipo de dirección IP en la creación

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

Para actualizar el tipo de dirección IP desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione la casilla de verificación del equilibrador de carga.
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. Elija Guardar cambios.

Para actualizar el tipo de dirección IP mediante el AWS CLI

Utilice el comando set-ip-address-type.

Grupos de seguridad para el equilibrador de carga de red

Puede asociar un grupo de seguridad a su equilibrador de carga de red para controlar el tráfico al que se permite llegar y dejar el equilibrador de carga. 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 a su equilibrador de carga, todo el tráfico de los clientes puede llegar a los oyentes del equilibrador de carga 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 a los clientes enviar tráfico a sus destinos a través del equilibrador de carga, pero evita que envíen tráfico directamente a los destinos. Hacer referencia al grupo de seguridad asociado a su equilibrador de carga de red en los grupos de seguridad asociados a los destinos garantiza que los destinos acepten el tráfico de su equilibrador de carga, incluso si habilita la preservación de la IP del cliente para su equilibrador de carga.

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

Contenido

- Actualizar los grupos de seguridad asociados
- Actualizar la configuración de seguridad
- Monitorear grupos de seguridad del equilibrador de carga

Consideraciones

- Puede asociar grupos de seguridad a un equilibrador de carga de red al crearlo. Si crea un equilibrador de carga de red sin asociar ningún grupo de seguridad, no podrá asociarlo al equilibrador de carga más adelante. Le recomendamos que asocie un grupo de seguridad al equilibrador de carga al crearlo.
- Después de crear un equilibrador de carga de red con los grupos de seguridad asociados, puede cambiar los grupos de seguridad asociados al equilibrador de carga 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 considera que los destinos se encuentan en mal estado.
- Puede controlar si el PrivateLink tráfico está sujeto a las reglas de entrada. Si habilita las reglas de entrada en el PrivateLink tráfico, el origen del tráfico es la dirección IP privada del cliente, no la interfaz del punto final.

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 interno, puede especificar un rango de CIDR de VPC como origen para permitir solo el tráfico de una VPC específica. Si se trata de un equilibrador de carga con acceso a Internet que debe aceptar tráfico desde cualquier lugar de Internet, puede especificar 0.0.0.0/0 como origen.

Entrada

Protocolo	Origen	Intervalo de puertos	Comentario
protocolo	*rango de direccion*	*puerto del oyente*	Permite el tráfico entrante desde el CIDR de origen en el puerto del oyente

Protocolo	Origen	Intervalo de puertos	Comentario
	es IP del cliente		
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 Path MTU Discovery en la Guía del usuario de Amazon EC2.

Salida

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

Ejemplo: Aceptar el tráfico solo desde el equilibrador de carga

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 tanto en el puerto de destino como en el de comprobación de estado. Para obtener más información, consulte the section called “Grupos de seguridad de destino”.

Entrada

Protocolo	Origen	Intervalo de puertos	Comentario
protocolo	sg-111112222233333	*puerto de destino*	Permite el tráfico entrante desde el equilibrador de carga en el puerto de destino

Protocolo	Origen	Intervalo de puertos	Comentario
protocolo	sg-111112 222233333	*comprobación de estado*	Permite el tráfico entrante desde el equilibrador de carga o el puerto de comprobación de estado

Salida

Protocolo	Destino	Intervalo de puertos	Comentario
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 cuando lo creó, puede actualizar los grupos de seguridad de ese equilibrador de carga en cualquier momento.

Para actualizar los grupos de seguridad desde la consola

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

Para actualizar los grupos de seguridad mediante el AWS CLI

Utilice el comando set-security-groups.

Actualizar la configuración de seguridad

De forma predeterminada, aplicamos las reglas del grupo de seguridad entrante a todo el tráfico que se envía al equilibrador de carga. Sin embargo, es posible que no desees aplicar estas reglas al tráfico que se envía al balanceador de cargas AWS PrivateLink, ya que puede provenir de direcciones IP superpuestas. En este caso, puedes configurar el balanceador de cargas para que no apliquemos las reglas de entrada al tráfico que se envía al balanceador de cargas a través de él. AWS PrivateLink

Para actualizar la configuración de seguridad a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibrio de carga), elija Load Balancers (Equilibradores de carga).
3. Seleccione el equilibrador de carga.
4. En la pestaña Seguridad, seleccione Editar.
5. En Configuración de seguridad, desactive la casilla Aplicar reglas de entrada al tráfico. PrivateLink
6. Elija Guardar cambios.

Para actualizar la configuración de seguridad mediante la AWS CLI

Utilice el comando set-security-groups.

Monitorear grupos de seguridad del equilibrador de carga

Utilice las `SecurityGroupBlockedFlowCount_Outbound` CloudWatch métricas `SecurityGroupBlockedFlowCount_Inbound` y para supervisar el recuento de flujos que están bloqueados por los grupos de seguridad del balanceador de cargas. El tráfico bloqueado no se refleja en otras métricas. Para obtener más información, consulte the section called “CloudWatch métricas”.

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

Etiquetas para el equilibrador de carga de red

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

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

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

Restricciones

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

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

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Tags (Etiquetas), elija Manage tags (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 valores nuevos en Clave y Valor.
7. Para eliminar una etiqueta, seleccione el botón Remove (Eliminar) junto a la etiqueta.
8. Cuando haya terminado, elija Guardar cambios.

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

Utilice los comandos add-tags y remove-tags.

Eliminar un equilibrador de carga de red

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

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

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

Cuando se elimina un balanceador de carga, se eliminan también sus agentes de escucha. Eliminar un balanceador de carga no afecta a los destinos registrados en él. Por ejemplo, las instancias EC2 continuarán ejecutándose y seguirán registradas en sus grupos de destino. Para eliminar los grupos de destino, consulte Eliminación de un grupo de destino.

Para eliminar un equilibrador de carga desde la consola

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

   Ejemplo:

   - Si el registro es un registro CNAME con un tiempo de vida (TTL) de 300 segundos, espere al menos 300 segundos antes de continuar con el siguiente paso.
   - Si el registro es un registro Alias (A) de Route 53, espere al menos 60 segundos.
   - Si utiliza Route 53, el cambio de registro tarda 60 segundos en propagarse a todos los servidores de nombres de Route 53 globales. Agregue este tiempo al valor de TTL del registro que se está actualizando.
2. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
3. En el panel de navegación, seleccione Equilibradores de carga.

4. Seleccione la casilla de verificación del equilibrador de carga.
5. Seleccione Acciones, Eliminar equilibrador de carga.
6. Cuando se le pida confirmación, ingrese **`confirm`** y elija Eliminar.

Para eliminar un balanceador de cargas mediante el AWS CLI

Utilice el comando delete-load-balancer.

Cambio de zona

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

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

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

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

- El equilibrio de carga entre zonas no se admite con cambios de zona. Debe desactivar el equilibrio de carga entre zonas para utilizar esta capacidad.
- El cambio de zona no se admite cuando se utiliza un Equilibrador de carga de aplicación como punto de conexión del acelerador en AWS Global Accelerator.
- Puede comenzar un cambio de zona para un equilibrador de carga específico solo para una zona de disponibilidad única. No puede comenzar un cambio de zona para varias zonas de disponibilidad.

- AWS elimina de forma proactiva las direcciones IP del balanceador de carga zonal del DNS cuando varios problemas de infraestructura afectan a los servicios. Compruebe siempre la capacidad actual de la zona de disponibilidad antes de comenzar un cambio de zona. Si sus equilibradores de carga tienen desactivado el equilibrio de carga entre zonas y utiliza un cambio de zona para eliminar la dirección IP del equilibrador de carga de zona, la zona de disponibilidad afectada por el cambio de zona también pierde la capacidad de destino.
- Cuando un Equilibrador de carga de aplicación sea el destino de un Equilibrador de carga de red, comience siempre el cambio de zona desde el Equilibrador de carga de red. Si comienza un cambio de zona desde el Equilibrador de carga de aplicación, el Equilibrador de carga de red no reconoce el cambio y continúa enviando tráfico al Equilibrador de carga de aplicación.

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

Comenzar un cambio de zona

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

Para comenzar un cambio de zona mediante la consola

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

   Todos los cambios de zona son temporales. Debe establecer un vencimiento, pero puede actualizar los cambios activos más adelante para establecer un vencimiento nuevo.

7. Ingrese un comentario. Si lo desea, puede actualizar el cambio de zona más adelante para editar el comentario.
8. Seleccione la casilla de verificación para confirmar que comenzar un cambio de zona reducirá la capacidad de su aplicación al cambiar el tráfico de la zona de disponibilidad.
9. Elija Iniciar.

Para iniciar un cambio zonal mediante el AWS CLI

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

Actualizar un cambio de zona

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

Para actualizar un cambio de zona mediante la consola

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

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

Para actualizar un cambio zonal mediante el AWS CLI

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

Cancelar un cambio de zona

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

Para cancelar un cambio de zona mediante la consola

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

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

Para cancelar un cambio zonal mediante el AWS CLI

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

Oyentes para 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
- 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 agente de escucha es TLS, debe implementar un único certificado de servidor SSL en el agente de escucha. Para obtener más información, consulte Agentes de escucha TLS del balanceador de carga de red.

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.

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.

En el caso de los equilibradores de carga de red de pila doble, solo se admiten los protocolos TCP y TLS.

Puede usarlo WebSockets con sus oyentes.

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.

Reglas del oyente

Al crear un oyente, debe especificar una regla para las solicitudes de redirección. Esta regla reenvíe las solicitudes al grupo de destino especificado. Para actualizar esta regla, consulte Actualizar un oyente para el equilibrador de carga de red.

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 regla del agente de escucha. 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 agente de escucha 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.

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.

Para agregar un agente de escucha a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, 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. En Protocolo, elija TCP, UDP, TCP_UDP o TLS. Deje el puerto predeterminado o especifique otro. En el caso de los equilibradores de carga de red de pila doble, solo se admiten los protocolos TCP y TLS.
6. En Acción predeterminada, elija un grupo de destino disponible.
7. [Agentes de escucha TLS] En Security policy (Política de seguridad), le recomendamos que mantenga la política de seguridad predeterminada.
8. [Agentes de escucha TLS] En Default SSL certificate (Certificado SSL predeterminado), realice una de las operaciones siguientes:
   - Si creó o importó un certificado utilizando AWS Certificate Manager, elija De ACM y elija el certificado.
   - Si ha cargado un certificado mediante IAM, elija Desde IAM y elija 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. Elija Add (Agregar).
11. [Agentes de escucha TLS] Para añadir una lista de certificados opcionales para utilizarla con el protocolo SNI, consulte Agregar certificados a la lista de certificados.

Para añadir un oyente mediante el AWS CLI

Utilice el comando create-listener para crear el agente de escucha.

Agentes de escucha TLS del balanceador de carga de red

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 front-end 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 renegociación de TLS ni la autenticación de TLS mutuo (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.

Para crear un agente de escucha TLS, consulte Añadir un agente de escucha. 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.

Certificados de servidor

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.

Como alternativa, puede utilizar las herramientas de TLS para crear una solicitud de firma de certificado (CSR) y, a continuación, conseguir que una CA firme la CSR para generar un certificado y, a continuación, importar el certificado a ACM o cargarlo en (IAM). AWS Identity and Access Management Para obtener más información, 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.

Contenido

Algoritmos clave compatibles

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

Políticas de seguridad

Al crear un agente de escucha TLS, debe seleccionar una política de seguridad. Puede actualizar la política de seguridad según sea necesario. Para obtener más información, consulte Actualizar la política de seguridad.

Consideraciones:

- La `ELBSecurityPolicy-TLS13-1-2-2021-06` política es la política de seguridad predeterminada para los oyentes de TLS creados con. AWS Management Console

  - Recomendamos la política de `ELBSecurityPolicy-TLS13-1-2-2021-06` seguridad, que incluye TLS 1.3 y es compatible con versiones anteriores de TLS 1.2.
- La `ELBSecurityPolicy-2016-08` política es la política de seguridad predeterminada para los oyentes de TLS creados con. AWS CLI
- Puede elegir la política de seguridad que se utilizará para las conexiones frontales, pero no para las conexiones finales.
  - En el caso de las conexiones de backend, si su oyente de TLS utiliza una política de seguridad de TLS 1.3, se utilizará la política de seguridad `ELBSecurityPolicy-TLS13-1-0-2021-06`. De lo contrario, la política de seguridad `ELBSecurityPolicy-2016-08` se utiliza con las conexiones de backend.
- Para cumplir con las normas de seguridad y conformidad que obligan a deshabilitar determinadas versiones del protocolo TLS, o para dar soporte a los clientes antiguos que requieren cifrados obsoletos, puede utilizar una de las políticas de seguridad. `ELBSecurityPolicy-TLS-` Puede habilitar los registros de acceso para obtener información sobre las solicitudes de TLS enviadas a su Network Load Balancer, analizar los patrones de tráfico de TLS, gestionar las actualizaciones de las políticas de seguridad y solucionar problemas. Habilita el registro de acceso para tu balanceador de cargas y examina 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.
- Puedes restringir las políticas de seguridad que están disponibles para los usuarios en todas tus políticas de IAM Cuentas de AWS y de control de servicios (SCP), respectivamente, y AWS Organizations mediante las claves de condición de Elastic Load Balancing. Para obtener más información, consulte las políticas de control de servicios (SCP) en la Guía del usuario AWS Organizations

Políticas de seguridad de TLS 1.3

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

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

- `ELBSecurityPolicy-TLS13-1-0-2021-06`
- `ELBSecurityPolicy-TLS13-1-3-2021-06`

Políticas de seguridad FIPS

El Estándar Federal de Procesamiento de la Información (FIPS) es un estándar gubernamental de EE. UU. y Canadá que especifica los requisitos de seguridad de los módulos criptográficos que protegen la información confidencial. Para obtener más información, consulte la Norma Federal de Procesamiento de Información (FIPS) 140 en la página sobre el cumplimiento de las normas de seguridad en la AWS nube.

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

Elastic Load Balancing proporciona las siguientes políticas de seguridad FIPS para Network Load Balancer:

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

Para las políticas admitidas

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

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

- ELBSecurityPolicy-FS-1-1-2019-08
- ELBSecurityPolicy-FS-2018-06

Políticas de seguridad de TLS 1.0 a 1.2

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

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

Protocolos y cifrados TLS

TLS 1.3

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

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

Ejemplo: La política de seguridad ELBSecurityPolicy-TLS13-1-2-2021-06 se muestra comoTLS13-1-2-2021-06.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Utilice el describe-ssl-policiescomando con cualquier política de seguridad de TLS 1.3.

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

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

FIPS

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

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

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

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

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

Políticas de seguridad	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256		✓	✓	✓	✓	✓	✓	✓

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

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

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

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

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

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

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
```

```
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

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

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

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

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

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

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

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

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

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

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

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

FS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TLS 1.0 - 1.2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

Cuando se actualiza el grupo de destino de la acción predeterminada del oyente, las conexiones nuevas se enrutan al grupo de destino recién configurado. 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.

Para actualizar el oyente desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir 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. Elija Editar.
6. (Opcional) Cambie los valores especificados en Protocolo y Puerto según sea necesario.
7. (Opcional) Elija un grupo de destino diferente para Acción predeterminada.
8. (Opcional) Agregue, actualice o elimine etiquetas según sea necesario.
9. Elija Guardar cambios.

Para actualizar el oyente mediante el AWS CLI

Utilice el comando modify-oyente.

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
- Agregar 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 agente de escucha TLS mediante el siguiente procedimiento. Para obtener más información, consulte Certificado predeterminado.

Para reemplazar el certificado predeterminado a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Load Balancers.
3. Seleccione el 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 Default SSL certificate (Certificado SSL predeterminado), realice una de las operaciones siguientes:
   - Si creó o importó un certificado utilizando AWS Certificate Manager, elija Desde ACM y elija el certificado.
   - Si ha cargado un certificado mediante IAM, elija Desde IAM y elija el certificado.
6. Elija Guardar cambios.

Para reemplazar el certificado predeterminado mediante el AWS CLI

Utilice el comando modify-listener con la opción --certificates.

Agregar 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 añadir uno o varios certificados. Como opción, añada el certificado predeterminado para asegurarse de que este certificado se utilice con el protocolo SNI incluso si se reemplaza como certificado predeterminado. Para obtener más información, consulte Lista de certificados.

Para añadir certificados a la lista de certificados utilizando la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, 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 casilla de verificación del oyente y elija Acciones, Agregar certificados SSL para el SNI.
6. Para agregar certificados que ya administra ACM o IAM, seleccione las casillas de verificación de los certificados y elija Incluir como pendiente a continuación.
7. Si cuenta con un certificado que no se encuentra administrado por ACM o IAM, elija Importar certificado, complete el formulario y elija Importar.
8. Elija Agregar certificados pendientes.

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

Utilice el comando add-listener-certificates.

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

Para quitar certificados de la lista de certificados utilizando la consola

1. 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 casilla de verificación del oyente y elija Acciones, Agregar certificados SSL para el SNI.
6. Active la casillas de los certificados y elija Remove (Eliminar).
7. Cuando se le solicite confirmación, ingrese **`confirm`** y elija Eliminar.

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

Utilice el comando remove-listener-certificates.

Actualizar la política de seguridad

Cuando 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 actualizar la política de seguridad a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione 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. Elija Editar.
6. En Security policy (Política de seguridad), seleccione una política de seguridad.
7. Elija Guardar cambios.

Para actualizar la política de seguridad mediante el AWS CLI

Utilice el comando modify-listener con la opción --ssl-policy.

Actualizar la política de ALPN

Puede actualizar la política de ALPN para el agente de escucha TLS a través del siguiente procedimiento. Para obtener más información, consulte Políticas de ALPN.

Para actualizar la política de ALPN a través de la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione 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. Elija Editar.
6. Para la política de ALPN, elija una política para habilitar ALPN o elija None (Ninguna) para deshabilitar ALPN.
7. Elija Guardar cambios.

Para actualizar la política de ALPN mediante el AWS CLI

Utilice el comando modify-listener con la opción --alpn-policy.

Eliminar un oyente de para el equilibrador de carga de red

Puede eliminar un oyente en cualquier momento.

Para eliminar un oyente a través de la consola

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

Para eliminar un oyente mediante el AWS CLI

Utilice el comando delete-listener.

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 los grupos de destino.

Contenido

- Equilibradores de carga de aplicación como destinos
- Etiquetas para su grupo de destino
- Eliminación de un grupo de destino

Configuración de enrutamiento

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

Los grupos de destino de los equilibradores de carga de red admiten los siguientes protocolos y puertos:

- Protocolos: TCP, TLS, UDP, TCP_UDP
- 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. Como el balanceador de cargas se encuentra en una nube privada virtual (VPC), el tráfico entre el balanceador de cargas y los destinos se autentica a nivel de paquete, por lo que no corre el riesgo man-in-the-middle de sufrir ataques o suplantación de identidad aunque los certificados de los destinos no sean válidos.

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	instance | ip	HTTP | HTTPS | TCP
TCP	TCP	alb	HTTP | HTTPS
TLS	TCP | TLS	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
UDP	UDP | TCP_UDP	instance | ip	HTTP | HTTPS | TCP
TCP_UDP	TCP_UDP	instance | ip	HTTP | HTTPS | TCP

Tipo de objetivo

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

> **Important**
>
> No puede especificar direcciones IP direccionables públicamente.

Todos los bloques de CIDR compatibles le permiten registrar los siguientes destinos en un grupo de destino:

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

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 de Amazon compartida (como participante), solo puede registrar los 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 Equilibradores de carga de aplicación como destinos.

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

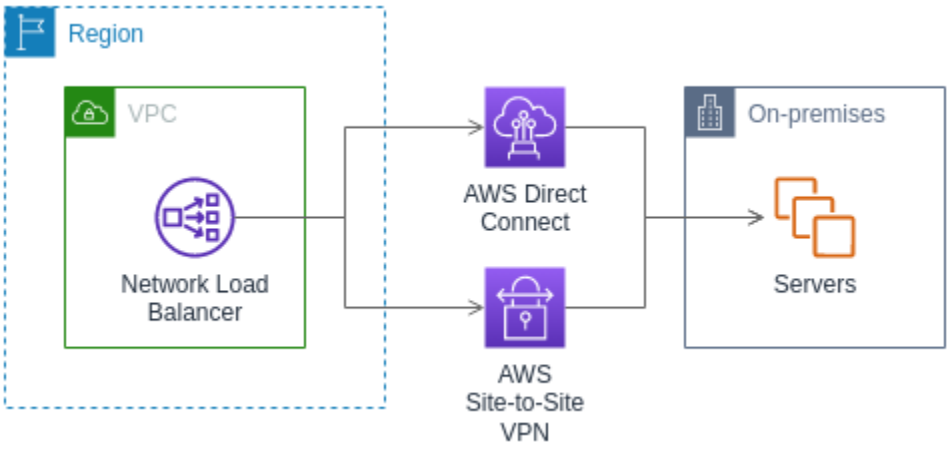
Si especifica destinos utilizando un ID de instancia, el tráfico se redirige a las instancias utilizando la dirección IP privada principal especificada en la interfaz de red principal de la instancia. El balanceador de carga vuelve a escribir la dirección IP de destino del paquete de datos antes de reenviarla 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 enlazados a través de una conexión VPN Site-to-Site AWS Direct Connect o una conexión VPN de sitio a sitio pueden servir como destino, si 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 AWS Direct Connect, consulte ¿Qué es? AWS Direct Connect

Para obtener más información AWS Site-to-Site VPN, consulte ¿Qué es 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 equilibradores de carga de red admiten grupos de destino de IPv4 e IPv6. La selección predeterminada es IPv4. Los grupos de destino de IPv6 solo se pueden asociar a los equilibradores de carga de red de pila doble.

Consideraciones

- Todas las direcciones IP de un grupo de destino deben tener el mismo tipo de dirección IP. Por ejemplo, no puede registrar un destino de IPv4 en un grupo de destino de IPv6.
- Los grupos de destino de IPv6 solo se pueden usar con equilibradores de carga de `dualstack` con oyentes de TLS o TCP.
- Los grupos de destino de IPv6 admiten destinos de tipo IP y de instancia.

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 balanceador de cargas comienza a enrutar el tráfico a un destino recién registrado tan pronto como se completa el proceso de registro y el objetivo pasa la primera comprobación de estado inicial, independientemente del umbral configurado.

Si la demanda de la aplicación se reduce o 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 las direcciones IPv6 en la Guía del usuario de Amazon EC2
- Al registrar los destinos por ID de instancia, las instancias deben estar en la misma VPC de Amazon 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 de UDP y TCP_UDP, no registre instancias por dirección IP si se encuentran fuera de la VPC del equilibrador de carga o si usan uno 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

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.

`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`.

`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. No se puede deshabilitar la preservación de IP de cliente para grupos de destino de UDP y TCP_UDP.

`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.

`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 es `off`, la conmutación por error de DNS está deshabilitada, lo que significa que cada grupo de destino

contribuye de forma independiente a la conmutación por error de DNS. El valor predeterminado de es 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

El porcentaje mínimo de destinos que deben estar en buen estado. Si el porcentaje de destinos en buen estado es inferior a este valor, marque la zona como zona en mal estado en DNS para que el tráfico se dirija solo a las zonas que están en buen estado. Los valores posibles son `off` o un número entero comprendido entre 1 y 100. Cuando es `off`, la conmutación por error de DNS está deshabilitada, lo que significa que cada grupo de destino contribuye de forma independiente a la conmutación por error de DNS. El valor predeterminado de es 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

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

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

El porcentaje mínimo de destinos que deben estar en buen estado. Si el porcentaje de destinos en buen estado es inferior a este valor, envíe el tráfico a todos los destinos, incluidos los destinos en mal estado. Los valores posibles son `off` o un número entero comprendido entre 1 y 100. El valor predeterminado es `off`.

`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`

El tiempo que tarda Elastic Load Balancing antes de cambiar el estado de un objetivo en mal estado de `unhealthy.draining` a`unhealthy`. El intervalo es de 0 a 360000 segundos. El valor predeterminado es 0 segundos.

Nota: Este atributo solo se puede configurar cuando `target_health_state.unhealthy.connection_termination.enabled` está. `false`

Preservación de la IP del cliente

Los equilibradores de carga de red pueden conservar la dirección IP de origen de los clientes al enrutar las solicitudes a los destinos de backend. Al deshabilitar la preservación de la IP del cliente, la dirección IP privada del equilibrador de carga de red se convierte en la dirección IP del cliente para todo el tráfico entrante.

De forma predeterminada, la preservación de la IP del cliente está habilitada (y no se puede deshabilitar) para los grupos de destino de tipo de IP y de instancia con los protocolos de UDP y TCP_UDP. 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 de IP (UDP, TCP_UDP): habilitados
- Grupos de destino de tipo de IP (TCP, TLS): deshabilitados

Requisitos y consideraciones

- Cuando la preservación de la IP del cliente está habilitada, los destinos deben estar en la misma VPC que el equilibrador de carga de red y el tráfico debe fluir directamente del equilibrador de carga de red al destino.
- La preservación de la IP del cliente no se admite cuando se usa un punto de conexión del equilibrador de carga de una puerta de enlace para inspeccionar el tráfico entre el equilibrador de carga de red y el destino (instancia o IP), incluso si el destino se encuentra en la misma VPC de Amazon 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 conservación de la IP del cliente no afecta al tráfico entrante procedente de AWS PrivateLink. La IP de origen del AWS PrivateLink tráfico es siempre la dirección IP privada del Network Load Balancer.

- No se admite la conservación de la IP del cliente cuando un grupo de destino contiene ENI de AWS PrivateLink o el ENI de otro equilibrador de carga de red. Esto provocará la 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 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.
- Los cambios en la preservación de la IP del cliente solo se aplican a las nuevas conexiones TCP.
- El bucle invertido de NAT, también conocido como horquilla, no se admite cuando la preservación de la IP del cliente está habilitada. Si está habilitada, es posible que se produzcan limitaciones en la conexión TCP/IP relacionadas con la reutilización observada de los sockets en los destinos. Estas limitaciones de conexión pueden producirse cuando un cliente o un dispositivo NAT situado delante del cliente utiliza la misma dirección IP y el mismo puerto de origen al conectarse a varios nodos del equilibrador de carga simultáneamente. Si el equilibrador de carga enruta estas conexiones al mismo destino, el destino ve las conexiones como si procedieran del mismo socket de origen, lo que provoca errores de conexión. Si esto ocurre, los clientes pueden volver a intentarlo (si la conexión falla) o volver a conectarse (si la conexión se interrumpe). Puede reducir este tipo de error de conexión aumentando la cantidad de puertos efímeros de origen o la cantidad de destinos para el equilibrador de carga. Puede evitar este tipo de error de conexión si deshabilita la preservación de la IP del cliente o el equilibrio de carga entre zonas.
- 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. Los errores de asignación de puertos se pueden rastrear mediante la métrica `PortAllocationErrorCount`. Para solucionar los errores de asignación de puertos, agregue más destinos al grupo de destino. Para obtener más información, consulte CloudWatch métricas para su Network Load Balancer.

Para configurar la conservación de la IP del cliente mediante la consola

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

2. En el panel de navegación, 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 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. Elija Guardar cambios.

Para activar o desactivar la conservación de la IP del cliente mediante el AWS CLI

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

Por ejemplo, use el siguiente comando para deshabilitar la preservación de la IP del cliente.

```
aws elbv2 modify-target-group-attributes --attributes
 Key=preserve_client_ip.enabled,Value=false --target-group-arn ARN
```

El resultado debería ser similar al siguiente ejemplo.

```
{
    "Attributes": [
      {
        "Key": "proxy_protocol_v2.enabled",
        "Value": "false"
      },
      {
        "Key": "preserve_client_ip.enabled",
        "Value": "false"
      },
      {
        "Key": "deregistration_delay.timeout_seconds",
        "Value": "300"
      }
    ]
}
```

Retardo de anulación del registro

Cuando se anula 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 en proceso de anulación del registro es `draining`. 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.

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.

Para actualizar los atributos de anulación del registro mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para 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. Elija Guardar cambios.

Para actualizar los atributos de anulación del registro mediante el AWS CLI

Utilice el comando modify-target-group-attributes.

Proxy Protocol

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 hay otra ruta de red para los destinos fuera del equilibrador de carga de red, el primer encabezado de protocolo de proxy podría no ser el de su equilibrador de carga de red.

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: las direcciones IP de origen son las direcciones IP privadas de los nodos del equilibrador de carga. Si necesita las direcciones IP de los clientes, habilite Proxy Protocol y obtenga dichas direcciones del encabezado Proxy Protocol.
- UDP y TCP_UDP: las direcciones IP de origen son las direcciones IP de los clientes.

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.

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

Servicios de punto de conexión de la 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.

Para habilitar Proxy Protocol v2 mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.

5. En la página Editar atributos, seleccione Proxy Protocol v2.
6. Elija Guardar cambios.

Para habilitar el protocolo proxy v2 mediante el AWS CLI

Utilice el comando modify-target-group-attributes.

Sesiones persistentes

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 adherencia está activado para un grupo objetivo, no se admiten las comprobaciones de estado pasivas. Para obtener más información, consulte Controles de salud para sus grupos objetivo.
- Los oyentes de TLS no admiten sesiones persistentes.

Para habilitar las sesiones sticky desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (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. Elija Guardar cambios.

Para habilitar las sesiones permanentes mediante el AWS CLI

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

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.

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

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 Reglas del oyente. 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 con el grupo de destino. También puede modificar la configuración de la comprobación de estado del grupo de destino. Para obtener más información, consulte Modificar la configuración de comprobación de estado de un grupo de destino.

Para crear un grupo de destino desde la consola

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

d. (Opcional) En Port, modifique el valor predeterminado según sea necesario.

e. En Tipo de dirección IP, elija IPv4 o IPv6. Esta opción solo está disponible si el tipo de destino son instancias o direcciones IP y el protocolo es TCP o TLS.

Debe asociar un grupo de destino de IPv6 a un equilibrador de carga de pila doble. Todos los destinos del grupo de destino deben tener el mismo tipo de dirección IP. No puede cambiar el tipo de dirección IP de un grupo de destino después de crearlo.

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 Comprobaciones de estado de los grupos de destino.
6. (Opcional) Para agregar una etiqueta, expanda Etiquetas, elija Agregar etiqueta e ingrese una clave y un valor de etiqueta.
7. Elija Siguiente.
8. En la página Registrar destinos, agregue uno o más destinos de la siguiente manera:

- Si el tipo de destino es Instancias, seleccione las instancias, ingrese los puertos y, a continuación, elija Incluir como pendiente a continuación.

Nota: Las instancias deben tener una dirección IPv6 principal asignada para poder registrarse en un grupo de destino de IPv6.

- Si el tipo de destino es Direcciones IP, seleccione la red, ingrese las direcciones IP y los puertos y, a continuación, seleccione Incluir como pendiente a continuación.

9. Elija Crear grupo de destino.

Para crear un grupo objetivo mediante el AWS CLI

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

Comprobaciones de estado de los grupos de destino

Puede registrar los destinos en uno o varios grupos de destino. El balanceador de carga comienza a redireccionar las solicitudes a un destino recién registrado tan pronto como finaliza el proceso de registro. 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 Equilibrio 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 y se dirigen a grupos con la adherencia activada. Para obtener más información, consulta Sesiones fijas.

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 balanceadores de carga de red también fallarán al abrirse si tienes un grupo objetivo 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 lo tanto, es posible que veas las conexiones TCP de esta prueba enviadas desde el balanceador de cargas a los destinos que están registrados en tu detector de TLS. Puede identificar estas conexiones TCP porque tienen la dirección IP de origen de su Network Load Balancer y las conexiones no contienen paquetes de datos.

En el caso de un servicio de UDP, la disponibilidad del destino se puede probar mediante comprobaciones de estado que no sean de UDP en el grupo de destino. Puede utilizar cualquier comprobación de estado disponible (TCP, HTTP o HTTPS) y cualquier puerto de su destino para verificar la disponibilidad de un servicio de UDP. 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 de un servicio de UDP, configure el servicio a la escucha del puerto de comprobación de estado a fin de realizar un seguimiento del estado de su servicio de UDP y fallar la comprobación de estado si el servicio no se encuentra disponible.

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 UnhealthyThresholdnúmero de errores consecutivos, el equilibrador de cargas deja el objetivo fuera de servicio. Cuando las comprobaciones de estado superan el HealthyThresholdnúmero de éxitos consecutivos, el equilibrador de cargas vuelve a poner el objetivo en servicio.

Opción	Descripción	Predeterminado
HealthCheckProtocolo	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
HealthCheckPuerto	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.
HealthCheckRuta	[Comprobaciones de estado HTTP/HTTPS] La ruta de comprobación de estado que es el destino de los controles 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 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.	6 segundos para las comprobaciones de estado de HTTP y 10 segundos para las comprobaciones de estado

Opción	Descripción	Predeterminado
		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. **Important** 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
HealthyThresholdCuenta	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

Opción	Descripción	Predeterminado
UnhealthyThresholdContar	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 objetivo no respondió a un chequeo de estado, no pasó el chequeo de estado o el objetivo está detenido. 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 objetivo no ha respondido a los controles de estado o no los ha superado y entra en un período de gracia. El objetivo admite las conexiones existentes y no aceptará ninguna conexión nueva durante este período 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 objetivo no se utiliza en una regla de escucha o el objetivo 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.
`Target.NotRegistered`	El destino no está registrado en el grupo de destino.

Comprobación del estado de los destinos

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

Para comprobar el estado de los destinos desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Elija el nombre del grupo de destino para abrir la página de detalles.
4. En el panel de Detalles se muestra el número total de destinos, más el número 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 comprobar el estado de tus objetivos, utiliza la AWS CLI

Utilice el comando describe-target-health. El resultado de este comando contiene el estado del destino. Incluye un código de motivo si el estado es cualquier valor distinto de `Healthy`.

Para recibir notificaciones por correo electrónico sobre destinos en mal estado

Utilice CloudWatch alarmas para activar una función Lambda que envíe detalles sobre objetivos en mal estado. Para step-by-step obtener instrucciones, consulta la siguiente entrada del blog: Cómo identificar los objetivos insalubres de tu balanceador de cargas.

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

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

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

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en 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 la configuración de la comprobación de estado, modifique la configuración según sea necesario y, a continuación, seleccione Guardar cambios.

Para modificar la configuración de las comprobaciones de estado de un grupo objetivo mediante el AWS CLI

Utilice el comando modify-target-group.

Equilibrio de carga entre zonas para grupos de destino

Los nodos del equilibrador de carga distribuyen las solicitudes procedentes de los clientes entre los destinos registrados. Cuando el equilibrio de carga entre zonas está habilitado, cada nodo del equilibrador de carga distribuye el tráfico entre los destinos registrados de todas las zonas de disponibilidad habilitadas. Cuando el equilibrio de carga entre zonas está deshabilitado, cada nodo del equilibrador de carga distribuye el tráfico únicamente entre los destinos registrados de su zona de disponibilidad. Esto 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 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.

Consideraciones

- Al habilitar el equilibrio de carga entre zonas para un Network Load Balancer, 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 AWS datos
- 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 esté desactivado, asegúrese de tener suficiente capacidad de destino en cada una de las zonas de disponibilidad del equilibrador de carga para que cada zona pueda atender su carga de trabajo asociada.

- Cuando el equilibrio de carga entre zonas esté 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.

Modificación del equilibrio de carga entre zonas en un equilibrador de carga

Puede activar o desactivar el equilibrio de carga entre zonas en el del equilibrador de carga en cualquier momento.

Modificación del equilibrio de carga entre zonas en un equilibrador de carga desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, 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. Elija Guardar cambios.

Para modificar el equilibrio de cargas entre zonas de tu balanceador de cargas mediante el AWS CLI

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

Modificación del equilibrio de carga entre zonas para un grupo de destino

La configuración del equilibrio de carga entre zonas a nivel del grupo de destino anula la configuración a nivel del equilibrador de carga.

Puede activar 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.

Modificación del equilibrio de carga entre zonas en un grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en 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. Elija Guardar cambios.

Para modificar el equilibrio de carga entre zonas para un grupo objetivo mediante el AWS CLI

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

Estado del grupo de destino

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

Acciones en mal estado

Puede configurar umbrales de buen estado para las siguientes acciones:

- Conmutación por error de DNS: cuando los destinos en buen estado de una zona están por debajo del umbral, marcamos las direcciones IP del nodo del equilibrador de carga de la zona como en mal estado en el DNS. Por lo tanto, cuando los clientes resuelven el nombre DNS del equilibrador de carga, el tráfico se enruta únicamente a las zonas en buen estado.
- Conmutación por error de enrutamiento: cuando los destinos en buen estado de una zona están por debajo del umbral, el equilibrador de carga envía tráfico a todos los destinos que están disponibles para el nodo del equilibrador de carga, incluidos los destinos en mal estado. Esto aumenta las probabilidades de que la conexión de un cliente se realice correctamente, en particular cuando los destinos no pasan temporalmente las comprobaciones de estado, y reduce el riesgo de sobrecargar los destinos en buen estado.

Requisitos y consideraciones

- 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 Equilibrio de carga entre zonas.
- Con la conmutación por error de DNS, eliminamos las direcciones IP de las zonas en mal estado del nombre de host DNS del equilibrador de carga. Sin embargo, la caché de DNS del cliente local puede contener estas direcciones IP hasta que caduque el time-to-live (TTL) del registro DNS (60 segundos).
- Cuando se produce una conmutación por error de DNS, esto afecta todos los grupos de destino asociados al equilibrador de carga. Asegúrese de tener suficiente capacidad en las zonas restantes para gestionar este tráfico adicional, especialmente si el equilibrio de carga entre zonas está desactivado.
- Con la conmutación por error de DNS, si se considera que todas las zonas del equilibrador de carga están en mal estado, el equilibrador de carga envía tráfico a todas las zonas, incluidas las zonas en mal estado.
- Existen otros factores, además de la existencia de suficientes destinos en buen estado, que podrían provocar una conmutación por error de DNS, como el estado de la zona.

Ejemplo

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

Escenario

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

Cuando el equilibrio de carga entre zonas está desactivado

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

Cuando el equilibrio de carga entre zonas está activado

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

de los destinos de los nodos del equilibrador de carga en ambas zonas de disponibilidad, lo que cumple con el porcentaje requerido de destinos en buen estado.

- El equilibrador de carga distribuye el tráfico entre los 14 destinos en buen estado en ambas zonas de disponibilidad.

Modificación de la configuración de estado de grupo de destino

Puede modificar la configuración del estado de grupo de destino de su grupo de destino de la siguiente manera.

Para modificar la configuración del estado de grupo de destino desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Compruebe si el equilibrio de carga entre zonas está activado o desactivado. Actualice esta configuración según sea necesario para asegurarse de que tiene suficiente capacidad para gestionar el tráfico adicional en caso de que falle una zona.
6. Amplíe los requisitos de estado del grupo de destino.
7. Para el tipo de configuración, le recomendamos que elija la configuración unificada, que establece el mismo umbral para ambas acciones.
8. Para conocer los requisitos para un buen estado, realice una de las siguientes acciones:
   - Elija Recuento mínimo de destinos en buen estado y, a continuación, introduzca un número entre 1 y el número máximo de destinos para su grupo de destino.
   - Elija el porcentaje mínimo de destinos en buen estado y, a continuación, introduzca un número del 1 al 100.
9. Elija Guardar cambios.

Para modificar la configuración de salud del grupo objetivo mediante el AWS CLI

Utilice el comando modify-target-group-attributes. En el siguiente ejemplo, se establece el umbral de buen estado para ambas acciones de mal estado en un 50 %.

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

```
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-
targets/73e2d6bc24d8a067 \
--attributes
 Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \

 Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

Interrupción de la conexión para destinos en mal estado

La terminación de la conexión está habilitada de forma predeterminada. Cuando el destino de un Network Load Balancer no pasa las comprobaciones de estado configuradas y se considera que está en mal estado, el balanceador de carga finaliza las conexiones establecidas y deja de enrutar las nuevas conexiones al destino. Si la terminación de la conexión está desactivada, se sigue considerando que el destino está en mal estado y no recibirá nuevas conexiones, pero las conexiones establecidas se mantienen activas, lo que permite que se cierren sin problemas.

La terminación de la conexión en el caso de los destinos en mal estado se puede configurar de forma individual para cada grupo objetivo.

Para modificar la configuración de interrupción de conexión desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Atributos, seleccione Editar.
5. 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. Elija Guardar cambios.

Para modificar la configuración de terminación de la conexión mediante el AWS CLI

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

Intervalo de drenaje insalubre

> **Important**
>
> La terminación de la conexión debe estar deshabilitada antes de habilitar un intervalo de drenaje incorrecto.

Los destinos en este `unhealthy.draining` estado se consideran en mal estado, no reciben nuevas conexiones, pero conservan las conexiones establecidas durante el intervalo configurado. El intervalo de conexión en mal estado determina la cantidad de tiempo que el objetivo permanece en el `unhealthy.draining` estado antes de que éste pase a serlo`unhealthy`. Si el objetivo pasa las comprobaciones de estado durante el intervalo de conexión en mal estado, su estado `healthy` vuelve a ser. Si se desencadena una anulación del registro, el estado del objetivo pasa a ser `draining` y comienza el tiempo de espera de la anulación del registro.

El intervalo de drenaje insalubre se puede configurar de forma individual para cada grupo objetivo.

Para modificar el intervalo de drenaje insalubre mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Atributos, seleccione Editar.
5. En Gestión del estado defectuoso de Target, asegúrese de que esté desactivada la opción Finalizar las conexiones cuando los destinos se deterioren.
6. Introduzca un valor para el intervalo de drenaje en mal estado.
7. Elija Guardar cambios.

Para modificar el intervalo de drenaje insalubre mediante el AWS CLI

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

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

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

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

Uso de Evaluate Target Health

- Cuando Evaluate Target Health se establece en `Yes` en un registro de alias para un equilibrador de carga de red, Route 53 evalúa el estado del recurso especificado por el valor de `alias target`. Para un equilibrador de carga de red, Route 53 utiliza las comprobaciones de estado del grupo de destino asociadas al equilibrador de carga.
- Cuando todos los grupos de destino de un equilibrador de carga de red están en buen estado, Route 53 marca el estado del registro de alias como en buen estado. Si un grupo de destino contiene al menos un destino en buen estado, se aprueba la comprobación de estado del grupo de destino. A continuación, Route 53 devuelve los registros de acuerdo con su política de enrutamiento. Si se utiliza la política de enrutamiento de conmutación por error, Route 53 devuelve el registro principal.
- Si alguno de los grupos de destino de un equilibrador de carga de red está en mal estado, el registro de alias no pasa la comprobación de estado de Route 53 (apertura por error). Si se utiliza la evaluación del estado del destino, no se aplicará la política de enrutamiento de conmutación por error.
- Si todos los grupos de destino de un equilibrador de carga de red están vacíos (no hay destinos), Route 53 considera que el registro está en mal estado (apertura por error). Si se utiliza la

evaluación del estado del destino, no se aplicará la política de enrutamiento de conmutación por error.

Para obtener más información, consulte Configuración de la conmutación por error de DNS en la Guía para desarrolladores de Amazon Route 53.

Registro de destinos con el grupo de destino

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 los grupos de destino.

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.

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 PrivateLink tráfico: si configuraste el balanceador de cargas para evaluar las reglas entrantes del tráfico que pasa AWS PrivateLink, agrega una regla que acepte el tráfico del grupo de seguridad del balanceador de cargas 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 PrivateLink el tráfico: agrega una regla que acepte el tráfico de las direcciones IP privadas del balanceador de cargas 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 los balanceadores

de carga de red de doble pila, preservamos las direcciones IP de los clientes al traducir las direcciones IPv4 a IPv6. Sin embargo, al traducir direcciones IPv6 a IPv4, la IP de origen siempre es la dirección IP privada del Network Load Balancer.

Para encontrar las direcciones IP privadas del balanceador de cargas mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, elija Interfaces de red.
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 Grupos de seguridad para el 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	Intervalo de puertos	Comentario
Direcciones IP de clientes	*oyente*	*oyente*	Permitir tráfico de cliente (tipo de destino `instance`)
CIDR DE VPC	*oyente*	*oyente*	Permitir tráfico de cliente (tipo de destino `ip`)

CIDR DE VPC	*comprobación de estado*	*comprobación de estado*	Permitir tráfico de comprobación de estado desde el balanceador de carga

Outbound

Destino	Protocolo	Intervalo de puertos	Comentario
Direcciones IP de clientes	*oyente*	*oyente*	Permitir respuestas a clientes (tipo de destino `instance`)
CIDR DE VPC	*oyente*	*oyente*	Permitir respuestas a clientes (tipo de destino `ip`)
CIDR DE VPC	*comprobación de estado*	1024 - 65535	Permitir tráfico de comprobación de estado

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	Intervalo de puertos	Comentario
Direcciones IP de clientes	*oyente*	*oyente*	Permitir tráfico de cliente (tipo de destino `instance`)
CIDR DE VPC	*oyente*	*oyente*	Permitir tráfico de cliente (tipo de destino `ip`)

CIDR DE VPC	*comprobación de estado*	1024 - 65535	Permitir tráfico de comprobación de estado

Outbound

Destino	Protocolo	Intervalo de puertos	Comentario
Direcciones IP de clientes	*oyente*	*oyente*	Permitir respuestas a clientes (tipo de destino `instance`)
CIDR DE VPC	*oyente*	*oyente*	Permitir respuestas a clientes (tipo de destino `ip`)
CIDR DE VPC	*comprobación de estado*	*comprobación de estado*	Permitir tráfico de comprobación de estado
CIDR DE VPC	*comprobación de estado*	1024 - 65535	Permitir tráfico de comprobación de estado

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.

Las subredes compartidas para los balanceadores de carga de red son compatibles en todas AWS las regiones, excepto:

- Asia-Pacífico (Osaka) `ap-northeast-3`
- Asia Pacífico (Hong Kong) `ap-east-1`

- Oriente Medio (Bahréin) `me-south-1`
- AWS China (Pekín) `cn-north-1`
- AWS China (Ningxia) `cn-northwest-1`

Registro o anulación del registro de 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 de su grupo de destino determina cómo se registran los destinos en ese grupo de destino. Para obtener más información, consulte Tipo de objetivo.

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 las direcciones IPv6 en la Guía del usuario de Amazon EC2
- Al registrar los destinos por ID de instancia, las instancias deben estar en la misma VPC de Amazon 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.
- En el caso de los grupos de destino de UDP y TCP_UDP, no registre instancias por dirección IP si se encuentran fuera de la VPC del equilibrador de carga o si usan uno 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.

Contenido

Registro o anulación del registro de destinos por ID de instancia

Una instancia debe tener el estado `running` al registrarla.

Para registrar un destino o anular su registro mediante el ID de instancia desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Para registrar instancias, elija Registrar destinos. Seleccione una o más instancias, ingrese el puerto de instancia predeterminado según sea necesario y, a continuación, elija Incluir como pendiente debajo. Cuando haya terminado de agregar instancias, elija Registrar destinos pendientes.

   Nota:

   - Las instancias deben tener una dirección IPv6 principal asignada para poder registrarse en un grupo de destino de IPv6.
   - AWS GovCloud (US) Region no admiten la asignación de una dirección IPv6 principal desde la consola. Debe usar la API para asignar direcciones IPv6 principales en s. AWS GovCloud (US) Region
6. Para anular el registro de instancias, seleccione la instancia y, a continuación, elija Anular registro.

Registro o anulación del registro de destinos por dirección IP

Destinos de IPv4

Una dirección IP que registre deben estar en uno de los siguientes bloques de CIDR:

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

- 192.168.0.0/16 (RFC 1918)

El tipo de dirección IP no se puede cambiar una vez que se creó el grupo de destino.

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

Destinos de IPv6

- Las direcciones IP que registre deben estar dentro del bloque de CIDR de VPC o dentro de un bloque de CIDR de VPC emparejado.
- El tipo de dirección IP no se puede cambiar una vez que se creó el grupo de destino.
- Solo puede asociar grupos de destino de IPv6 a un equilibrador de carga de pila doble con oyentes de TCP o TLS.

Para registrar un destino o anular su registro mediante la dirección IP desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Para registrar direcciones IP, elija Registrar destinos. Para cada dirección IP, especifique la red, la zona de disponibilidad, la dirección IP (IPv4 o IPv6) y el puerto y, a continuación, elija Incluir como pendiente a continuación. Cuando haya terminado de especificar direcciones, elija Registrar destinos pendientes.
6. Para anular el registro de direcciones IP, selecciónelas y, a continuación, elija Anular registro. Si ha registrado muchas direcciones IP, puede que le resulte útil agregar un filtro o cambiar el orden.

Registro o anulación del registro de destinos mediante la AWS CLI

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

Equilibradores de carga de aplicación como destinos

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

- Para asociar un Application Load Balancer como destino de un Network Load Balancer, deben estar en la misma Amazon VPC dentro de la misma cuenta.
- Puede asociar un equilibrador de carga de aplicación como destino de varios equilibradores de carga de red. Para ello, registre el equilibrador de carga de aplicación con un grupo de destino diferente para cada equilibrador de carga de red individual.
- Cada equilibrador de carga de aplicación que registre en un equilibrador de carga de red reduce la cantidad máxima de destinos por zona de disponibilidad por equilibrador de carga de red en 50 (si el equilibrio de carga entre zonas está deshabilitado) o 100 (si el equilibrio de carga entre zonas está habilitado). 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.

Paso 1: crear un equilibrador de carga de aplicación

Antes de empezar, configure los grupos de destino que utilizará este equilibrador de carga de aplicación. Asegúrese de tener una nube privada virtual (VPC) con los destinos que registrará en el grupo de destino. Esta VPC debe tener al menos una subred pública en al menos una de las zonas de disponibilidad utilizadas por los destinos.

Para crear un Application Load Balancer mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En 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 aplicación, elija Create (Crear).
5. En la página Crear equilibrador de carga de aplicación, en Configuración básica, especifique el Nombre del equilibrador de carga, el Esquema y el Tipo de dirección IP.
6. Para Oyentes, puede crear un oyente HTTP o HTTPS en cualquier puerto. Sin embargo, debe asegurarse de que el número de puerto de este oyente coincida con el puerto del grupo de destino en el que residirá este equilibrador de carga de aplicación.
7. En Zonas de disponibilidad, haga lo siguiente:

   a. Para la VPC, seleccione una nube privada virtual (VPC) con instancias o direcciones IP que haya incluido como destinos de su equilibrador de carga de aplicación. Debe usar la misma VPC que usaría para su equilibrador de carga de red en Paso 3: crear un equilibrador de carga de red y configurar el equilibrador de carga de aplicación como su destino.

   b. Seleccione dos o más zonas de disponibilidad y las subredes correspondientes. Asegúrese de que estas zonas de disponibilidad coincidan con las habilitadas para su equilibrador de carga de red a fin de optimizar la disponibilidad, el escalado y el rendimiento.
8. Puede asignar un grupo de seguridad a su equilibrador de carga mediante la creación de un grupo de seguridad nuevo o la selección de uno existente.

   Este grupo de seguridad que seleccione debe contener una regla que permita dirigir el tráfico al puerto de oyente para este equilibrador de carga. Utilice los bloques de CIDR (intervalo de direcciones IP) de los ordenadores del cliente como fuente de tráfico en las reglas de entrada de los grupos de seguridad. Esto permite que los clientes envíen tráfico a través de este equilibrador de carga de aplicación. Para obtener más información sobre cómo

configurar grupos de seguridad para un equilibrador de carga de aplicación como destino de un equilibrador de carga de red, consulte Grupos de seguridad para el equilibrador de carga de aplicación en la Guía del usuario de equilibradores de carga de aplicación.

9. En Configurar enrutamiento, seleccione el grupo de destino que configuró para este equilibrador de carga de aplicación. Si no tiene un grupo de destino disponible y desea configurar uno nuevo, consulte Crear un grupo de destino en la Guía del usuario de los equilibradores de carga de aplicaciones.
10. Revise la configuración y elija Create load balancer (Crear equilibrador de carga).

Para crear el Application Load Balancer mediante el AWS CLI

Utilice el comando create-load-balancer.

Paso 2: crear el grupo de destino con el equilibrador de carga de aplicación como destino

Crear un grupo de destino le permite registrar un equilibrador de carga de aplicación nuevo o existente como destino. Solo puede agregar un equilibrador de carga de aplicación por grupo de destino. El mismo equilibrador de carga de aplicación también se puede usar en un grupo de destino separado, como destino de hasta dos equilibradores de carga de red.

Para crear un grupo objetivo y registrar el Application Load Balancer como destino, mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija Crear grupo de destino.
4. En la página Especificar detalles del grupo, en Configuración básica, elija Equilibrador de carga de aplicación.
5. En Nombre del grupo de destino, escriba el nombre del grupo de destino del equilibrador de carga de aplicación.
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 de oyente de equilibrador de carga de aplicación. Como alternativa, puede agregar o editar el puerto de oyente en el equilibrador de carga de aplicación para que coincida con este puerto.

7. En VPC, seleccione la nube privada virtual (VPC) con el equilibrador de carga de aplicación que desee registrar con el grupo de destino.
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) Agregue una o varias etiquetas según sea necesario.
10. Elija Siguiente.
11. En la página Registrar destinos, elija el equilibrador de carga de aplicación que desee registrar como destino. El equilibrador de carga de aplicación que elija de la lista debe tener un oyente en el mismo puerto que el grupo de destino que va a crear. Puede agregar o editar un oyente en este equilibrador de carga para que coincida con el puerto del grupo de destino o volver al paso anterior y cambiar el puerto especificado para el grupo de destino. Si no está seguro de qué equilibrador de carga de aplicación debe agregar como destino o no quiere agregarlo en este momento, puede optar por agregar el equilibrador de carga de aplicación más adelante.
12. Elija Crear grupo de destino.

Para crear un grupo de destino y registrar el equilibrador de carga de aplicación como destino mediante la AWS CLI

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

Paso 3: crear un equilibrador de carga de red y configurar el equilibrador de carga de aplicación como su destino

Siga los pasos siguientes para crear el equilibrador de carga de red y, a continuación, configure el equilibrador de carga de aplicación como su destino desde la consola.

Para crear el Network Load Balancer y el listener mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibrio de carga), elija Load Balancers (Equilibradores de carga).
3. Elija Crear un equilibrador de carga.

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

   En el panel de Configuración básica, configure el Nombre del equilibrador de carga, el Esquema y el Tipo de dirección IP.
6. Asignación de redes

   a. En VPC, seleccione la misma VPC que utilizó para el destino del equilibrador de carga de aplicación. Si seleccionó Con acceso a Internet en Esquema, solo se pueden seleccionar las VPC con una puerta de enlace de Internet.

   b. En Asignaciones, seleccione dos o más zonas de disponibilidad y las subredes correspondientes. Le recomendamos que seleccione las mismas zonas de disponibilidad que el destino del equilibrador de carga de aplicación para optimizar 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. 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. Como Acción predeterminada, seleccione el grupo de destino del equilibrador de carga de aplicación para redirigir el tráfico. Si no lo ve en la lista o no puede seleccionar un grupo de destino (porque ya lo está utilizando otro equilibrador de carga de red), puede crear un grupo de destino del equilibrador de carga de aplicación como se muestra en Paso 2: crear el grupo de destino con el equilibrador de carga de aplicación como destino.
8. Etiquetas

   (Opcional) Agregue etiquetas para categorizar su equilibrador de carga. Para obtener más información, consulte Etiquetas.

9. Resumen

   Revise la configuración y elija Create load balancer (Crear equilibrador de carga).

Para crear el Network Load Balancer mediante el AWS CLI

Utilice el comando create-load-balancer.

Paso 4: (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 .

Etiquetas para su grupo de destino

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

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

Cuando ya no necesite una etiqueta, puede eliminarla.

Restricciones

- Número máximo de etiquetas por recurso: 50

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

Para actualizar las etiquetas de un grupo objetivo mediante la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, en Load Balancing (Equilibración de carga), elija Target Groups (Grupos de destino).
3. Elija el nombre del grupo de destino para mostrar su página de detalles.
4. En la pestaña Etiquetas, elija Administrar etiquetas y realice una o varias de las acciones siguientes:
   a. Para actualizar una etiqueta, ingrese valores nuevos para Clave y Valor.
   b. Para añadir una etiqueta, seleccione Agregar etiqueta y escriba una Clave y un Valor.
   c. Para eliminar una etiqueta, elija Eliminar junto a la etiqueta.
5. Cuando haya terminado de actualizar las etiquetas, elija Guardar cambios.

Para actualizar las etiquetas de un grupo objetivo mediante el AWS CLI

Utilice los comandos add-tags y remove-tags.

Eliminación de un grupo de destino

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

Para eliminar un grupo objetivo mediante la consola

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

2. En el panel de navegación, en Equilibrio de carga, elija Grupos de destino.
3. Seleccione el grupo de destino y elija Actions, Delete.
4. Cuando se le indique que confirme, seleccione Sí, borrar.

Para eliminar un grupo objetivo mediante el AWS CLI

Utilice el comando delete-target-group.

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.

CloudWatch métricas

Puedes usar Amazon CloudWatch para recuperar estadísticas sobre puntos de datos para tus balanceadores de carga y objetivos como un conjunto ordenado de datos de series temporales, conocidos como métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte CloudWatch métricas para su Network Load Balancer.

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.

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.

CloudTrail registros

Se puede utilizar AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a la API de Elastic Load Balancing y almacenarlas como archivos de registro en Amazon S3. Puede usar estos CloudTrail registros para determinar qué llamadas se realizaron, la dirección IP de origen de la llamada, quién realizó la llamada, cuándo se realizó la llamada, etc. Para obtener más información, consulte Registro de llamadas a la API del equilibrador de carga de red mediante AWS CloudTrail.

CloudWatch métricas para su Network Load Balancer

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

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una CloudWatch alarma para supervisar una métrica específica e iniciar una acción (como enviar una notificación a una dirección de correo electrónico) si la métrica se encuentra fuera de lo que considera un rango aceptable.

Elastic Load Balancing CloudWatch solo informa de las métricas cuando las solicitudes fluyen a través del balanceador de carga. Si hay solicitudes fluyendo a través del equilibrador de carga, Elastic Load Balancing mide y envía las métricas a intervalos de 60 segundos. Si no fluye ninguna solicitud a través del equilibrador de carga o no hay datos para una métrica, esta no se notifica. En el caso de los balanceadores de carga de red con grupos de seguridad, el tráfico rechazado por los grupos de seguridad no se captura en las CloudWatch métricas.

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

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`
`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

Métrica	Descripción
	Estadísticas: las estadísticas más útiles son `Average`, `Maximum` y `Minimum`. Dimensiones • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`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`
`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`

Métrica	Descripción
`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`
`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`

Métrica	Descripción
`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`
`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`

Métrica	Descripción
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 del informe: indica si se han activado las comprobaciones de estado. 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
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

Métrica	Descripción
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
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
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: hay un valor distinto de cero. Estadísticas: la estadística más útil es Maximum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer

Métrica	Descripción
`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: hay un valor distinto de cero. Estadísticas: la estadística más útil es `Sum`. Dimensiones • `LoadBalancer` • `AavailabilityZone` , `LoadBalancer`
`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`

Métrica	Descripción
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
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

Métrica	Descripción
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: hay un valor distinto de cero. Estadísticas: la estadística más útil es Sum. Dimensiones • LoadBalancer • AvailabilityZone , LoadBalancer
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

Métrica	Descripción
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
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

Métrica	Descripción
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
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 • AvailabilityZone , LoadBalancer

Métrica	Descripción
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
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

Métrica	Descripción
`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 del informe: indica si se han activado las comprobaciones de estado. 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). Criterios del informe: hay un valor distinto de cero. 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.

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

Las estadísticas `Minimum` y `Maximum` reflejan los valores mínimo y máximo de los puntos de datos registrados en los nodos individuales del equilibrador de carga en cada ventana de muestreo. 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.

Vea CloudWatch las métricas de su balanceador de carga

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

Como alternativa, puede ver las métricas de su balanceador de carga mediante la consola. CloudWatch

Para consultar las métricas desde la consola de

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Para ver las métricas filtradas por grupo de destino, haga lo siguiente:
   a. En el panel de navegación, elija Target Groups.
   b. Seleccione el grupo de destino y 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 ver las métricas mediante la consola CloudWatch

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.

3. Seleccione el espacio de nombres NetworkELB.
4. (Opcional) Para ver una métrica en todas las dimensiones, escriba su nombre en el campo de búsqueda.

Para ver las métricas mediante 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 mediante el 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 única de dimensiones como una métrica independiente. No se pueden recuperar estadísticas utilizando combinaciones de dimensiones que no se han publicado expresamente. Debe especificar las mismas dimensiones que se utilizaron al crear las métricas.

```
aws cloudwatch get-metric-statistics --namespace AWS/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 Network Load Balancer. Puede utilizar estos registros de acceso para analizar los patrones de tráfico y solucionar problemas.

> **Important**
>
> Los registros de acceso se crean solo cuando el Network Load Balancer tiene un detector de TLS y contienen información únicamente sobre las conexiones TLS.

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 KMS que se rota periódicamente. Para obtener más información, consulte Especificar el cifrado de Amazon S3 (SSE-S3) y Especificar el cifrado del lado del servidor con AWS KMS (SSE-KMS) en la Guía del usuario de Amazon S3.

Los logs 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.

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

Nombre del bucket de S3.

prefix

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 del propietario. Cuenta de AWS

region

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

aaaa/mm/dd

La fecha de entrega del log.

load-balancer-id

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

end-time

La fecha y hora en que finalizó el intervalo de registro. Por ejemplo, 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
type	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.
oyente	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.

Campo	Descripción
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.
received_bytes	Número de bytes recibidos por el balanceador de carga desde el cliente después del descifrado.
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 -.

Campo	Descripción
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 -.
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
```

Requisitos del bucket

Al habilitar el registro de acceso, es preciso especificar un bucket de S3 para los logs de acceso. El bucket puede pertenecer a otra cuenta que no sea la propietaria del balanceador de carga. El bucket debe cumplir los siguientes requisitos.

Requisitos

- El bucket debe estar ubicado en la misma región que el equilibrador de carga.
- 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. A continuación, se muestra una política de ejemplo.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::my-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:::my-bucket/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:*"]
                }
            }
        }
    ]
}
```

En la política anterior, para `aws:SourceAccount`, especifique la lista de números de cuenta para los que se entregan los registros a este bucket. Para `aws:SourceArn`, especifique la lista de ARN del recurso que genera los registros, en el formulario `arn:aws:logs:`*`source-region`*`:`*`source-account-id`*`:*`.

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)
- AWS KMS claves almacenadas en AWS Key Management Service (SSE-KMS) †

† Con los registros de acceso de Network Load Balancer, no puede usar claves AWS administradas, debe usar claves administradas por el cliente.

Para obtener más información, consulte Especificar el cifrado de Amazon S3 (SSE-S3) y Especificar el cifrado del lado 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.

```
{
  "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": "*"
    }
  ]
}
```

Habilitar el registro de acceso

Al habilitar el registro de acceso del equilibrador de carga, debe especificar el bucket de S3 donde el equilibrador de carga almacenará los registros. Asegúrese de que posee este bucket y de que ha configurado la política de bucket correspondiente para este bucket. Para obtener más información, consulte Requisitos del bucket.

Para habilitar el registro de acceso desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione 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 Edit load balancer attributes, lleve a cabo alguna de las siguientes operaciones:

    a. Para la supervisión, active los registros de acceso.

b. Seleccione Explorar S3 y seleccione el bucket que quiera usar. También puede introducir la ubicación del bucket de S3, incluido cualquier prefijo.

c. Elija Guardar cambios.

Para habilitar el registro de acceso mediante AWS CLI

Utilice el comando modify-load-balancer-attributes.

Deshabilitar el registro de acceso

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

Para deshabilitar el registro de acceso desde la consola

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Equilibradores de carga.
3. Seleccione el nombre del equilibrador de carga para abrir la página de detalles.
4. En la pestaña Atributos, seleccione Editar.
5. Para la Monitorización, desactive los registros de acceso.
6. Elija Guardar cambios.

Para deshabilitar el registro de acceso mediante el AWS CLI

Utilice el comando modify-load-balancer-attributes.

Procesamiento de archivos de registro de acceso

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

Si existe una gran cantidad de demanda en el sitio web, el equilibrador de carga puede generar archivos registro con gigabytes de datos. Es posible que no pueda procesar una cantidad tan grande de datos mediante el line-by-line procesamiento. En tal caso, podría ser preciso utilizar herramientas

de análisis que ofrezcan soluciones de procesamiento en paralelo. Por ejemplo, puede utilizar las siguientes herramientas de análisis para analizar y procesar los registros de acceso:

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

Registro de llamadas a la API del equilibrador de carga de red mediante AWS CloudTrail

Elastic Load Balancing está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS en Elastic Load Balancing. CloudTrail captura todas las llamadas a la API de Elastic Load Balancing como eventos. Las llamadas capturadas incluyen llamadas desde AWS Management Console y llamadas de código a las operaciones de la API de Elastic Load Balancing. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Elastic Load Balancing. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Elastic Load Balancing, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre Elastic Load Balancing en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Elastic Load Balancing, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos en su entorno Cuenta de AWS, incluidos los eventos de Elastic Load Balancing, cree una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la

consola, la ruta se aplica a todas AWS las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otras Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos. Para más información, consulte los siguientes temas:

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

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

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

- Si la solicitud se realizó con las credenciales raíz o del usuario.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte el elemento CloudTrailUserIdentity.

Descripción de las entradas del archivo de registros de Elastic Load Balancing

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera, y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un seguimiento ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

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

A continuación, se muestran ejemplos de CloudTrail registros de Elastic Load Balancing para un usuario que creó un Network Load Balancer y, a continuación, lo eliminó mediante. AWS CLI Puede identificar la CLI mediante los elementos `userAgent`. Puede identificar las llamadas al API solicitadas mediante los `eventName`. Encontrará la información sobre el usuario (`Alice`) en el elemento `userIdentity`.

Example Ejemplo: CreateLoadBalancer


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing",
        "type": "network"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "network",
            "ipAddressType": "ipv4",
```

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

Example Ejemplo: DeleteLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
```

```
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Solución de problemas 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 los grupos de destino.

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

Hay un grupo de seguridad que no permite el tráfico

> 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.

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.

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.

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 un cliente de un equilibrador de carga que está registrado y tiene activada la preservación de IP de cliente, la conexión solo se realizará correctamente si la solicitud se enruta a otra instancia. 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.

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
- 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 al conectarse a través de AWS PrivateLink

Si el equilibrador de carga de red está asociado con un servicio de punto de conexión de VPC, admitirá 55 000 conexiones simultáneas o unas 55 000 conexiones por minuto con cada uno de los distintos destinos (dirección IP y puerto). Si se superan estas conexiones, el riesgo de que se produzcan errores de asignación de puertos será mayor. Los errores de asignación de puertos se pueden rastrear mediante la métrica `PortAllocationErrorCount`. Para solucionar los errores de asignación de puertos, agregue más destinos al grupo de destino. Para obtener más información, consulte CloudWatch métricas para su Network Load Balancer.

Fallo de conexión intermitente cuando la preservación de IP del cliente está habilitada

Si la preservación de la IP del cliente está habilitada, es posible que se produzcan limitaciones en la conexión TCP/IP relacionadas con la reutilización observada de los sockets en los destinos. Estas limitaciones de conexión pueden producirse cuando un cliente, o un dispositivo NAT situado delante del cliente, utiliza la misma dirección IP y el mismo puerto de origen al conectarse a varios nodos del equilibrador de carga simultáneamente. Si el equilibrador de carga enruta estas conexiones al mismo destino, el destino ve las conexiones como si procedieran del mismo socket de origen, lo que provoca errores de conexión. Si esto ocurre, los clientes pueden volver a intentarlo (si la conexión falla) o volver a conectarse (si la conexión se interrumpe). Puede reducir este tipo de error de conexión aumentando la cantidad de puertos efímeros de origen o la cantidad de destinos para el equilibrador de carga. Puede evitar este tipo de error de conexión si deshabilita la preservación de la IP del cliente o el equilibrio de carga entre zonas.

Además, cuando la preservación de la IP del cliente está habilitada, la conectividad puede fallar si los clientes que se conectan al equilibrador de carga de red también están conectados a los destinos situados detrás del equilibrador de carga. Para solucionar este problema, puede deshabilitar la preservación de la IP del cliente en los grupos de destino afectados. Como alternativa, haga que sus clientes se conecten solo al equilibrador de carga de red o solo a los destinos, pero no a ambos.

Retrasos en la conexión TCP

Cuando se habilitan tanto el equilibrio de carga entre zonas como la preservación de la IP del cliente, un cliente que se conecte a diferentes IP del mismo equilibrador de carga puede enrutarse al mismo destino. Si el cliente usa el mismo puerto de origen para ambas conexiones, el destino recibirá lo que parece ser una conexión duplicada, lo que puede provocar errores de conexión y demoras en el TCP a la hora de establecer nuevas conexiones. Puede evitar este tipo de error de conexión si deshabilita el equilibrio de carga entre zonas. Para obtener más información, consulte Equilibrio de carga entre zonas.

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.

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.

Solucione los problemas de los objetivos en mal estado mediante el mapa de recursos

Si los objetivos de Network Load Balancer no superan las comprobaciones de estado, puede utilizar el mapa de recursos para encontrar los objetivos en mal estado y tomar medidas en función del código del motivo del error. Para obtener más información, consulte Mapa de recursos de Network Load Balancer.

El mapa de recursos ofrece dos vistas: vista general y mapa objetivo en mal estado. La vista general está seleccionada de forma predeterminada y muestra todos los recursos del balanceador de cargas. Al seleccionar la vista Mapa de objetivos en mal estado, solo se mostrarán los objetivos en mal estado de cada grupo de objetivos asociado al Network Load Balancer.

> **Note**
>
> La opción Mostrar detalles de los recursos 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 activado, debe seleccionar cada recurso para ver sus detalles.

La columna Grupos objetivo muestra un resumen de los objetivos saludables y no saludables de cada grupo objetivo. Esto puede ayudar a determinar si todos los objetivos están fallando en los controles de estado o solo algunos objetivos específicos están fallando. Si todos los objetivos de un grupo objetivo no pasan los controles de estado, compruebe la configuración de los controles de estado del grupo objetivo. Seleccione el nombre de un grupo objetivo para abrir su página de detalles en una pestaña nueva.

La columna TargetID muestra el TargetID y el estado actual de la comprobación de estado de cada objetivo. Cuando un objetivo no está en buen estado, se muestra el código del motivo del error en la comprobación de estado. Cuando un solo objetivo no supere una comprobación de estado, compruebe que el objetivo tiene recursos suficientes. Selecciona el ID de un objetivo para abrir su página de detalles en una pestaña nueva.

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

Compruebe que su instancia no supere las comprobaciones de estado y, a continuación, compruebe el código del motivo de la falla para detectar los siguientes problemas:

- Incorrecto: se agotó el tiempo de espera de la solicitud
  - Compruebe que los grupos de seguridad y las listas de control de acceso a la red (ACL) asociados a sus objetivos y a Network Load Balancer no bloqueen la conectividad.
  - Compruebe que el destino tenga suficiente capacidad disponible para aceptar conexiones desde el Network Load Balancer.
  - Las respuestas a las comprobaciones de estado del balanceador de carga de red se pueden ver en los registros de aplicaciones de cada destino. Para obtener más información, consulta los códigos de motivo de Health Check.
- Insalubre: FailedHealthChecks
  - Compruebe que el objetivo esté escuchando el tráfico en el puerto de comprobación de estado.

    > **Cuando se utiliza un detector de TLS**
    >
    > Usted elige qué política de seguridad se utilizará para las conexiones front-end. La política de seguridad utilizada para las conexiones de back-end se selecciona automáticamente en función de la política de seguridad de front-end que se utilice.
    >
    > - Si su agente de escucha de TLS utiliza una política de seguridad de TLS 1.3 para las conexiones de front-end, la política de seguridad se utiliza para las conexiones de back-end. `ELBSecurityPolicy-TLS13-1-0-2021-06`
    > - Si su agente de escucha de TLS no utiliza una política de seguridad de TLS 1.3 para las conexiones de front-end, la política de seguridad se utilizará para las conexiones de back-end. `ELBSecurityPolicy-2016-08`
    >
    > Para obtener más información, consulte Políticas de seguridad.

  - Compruebe que el destino proporciona un certificado y una clave de servidor en el formato correcto especificado en la política de seguridad.
  - Compruebe que el destino admita uno o más cifrados coincidentes y un protocolo proporcionado por el Network Load Balancer 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, utilice el formulario de aumento del límite de Elastic Load Balancing.

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
Grupos de destino por acción y por equilibrador de carga de red	1	No
Destinos por zona de disponibilidad por equilibrador de carga de red	500 [2, 3]	Sí
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 los grupos de destinos.

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.

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
Certificados RSA de 3072 bits y ECDSA de 256/384/521 bits	Esta versión añade compatibilidad con los certificados RSA de 3072 bits y los certificados del algoritmo de firma digital de curva elíptica (ECDSA) de 256, 384 y 521 bits mediante (ACM). AWS Certificate Manager	19 de enero de 2024
Terminación TLS FIPS 140-3	Esta versión añade políticas de seguridad que utilizan módulos criptográficos FIPS 140-3 al finalizar las conexiones TLS.	20 de noviembre de 2023
Afinidad de DNS zonal	En esta versión, se añade la compatibilidad con los 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
Desactive la terminación de la conexión de destino en mal	Esta versión añade compatibilidad para mantener las conexiones activas con los destinos que no pasen las comprobaciones de estado.	12 de octubre de 2023
Terminación de la conexión UDP predeterminada	De forma predeterminada, esta versión permite finalizar	12 de octubre de 2023

	las conexiones UDP al finalizar el tiempo de espera de la cancelación del registro.	
Registre los destinos mediante IPv6	Esta versión añade compatibilidad con el registro de instancias como destinos cuando se direcciona 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 añade soporte para configurar el equilibrio de carga entre zonas a nivel del grupo objetivo.	17 de noviembre de 2022
Grupos de destino IPv6	Esta versión agrega soporte para configurar grupos de destino de IPv6 para los balanceadores de carga de red.	23 de noviembre de 2021

Equilibradores de carga internos de IPv6	Esta versión añade compatibilidad con la configuración de grupos de destino de IPv6 para los balanceadores 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	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 añade compatibilidad con tres políticas de seguridad adicionales predefinidas de confidencialidad directa.	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
Disponible en una nueva región	Esta versión añade compatibilidad con los balanceadores de carga de red en la región de 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

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.