## Elastic Load Balance

# Guía del usuario

**Edición** 01

**Fecha** 2025-08-22

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

## Marcas registradas y permisos

El logotipo HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

## Aviso

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

# Índice



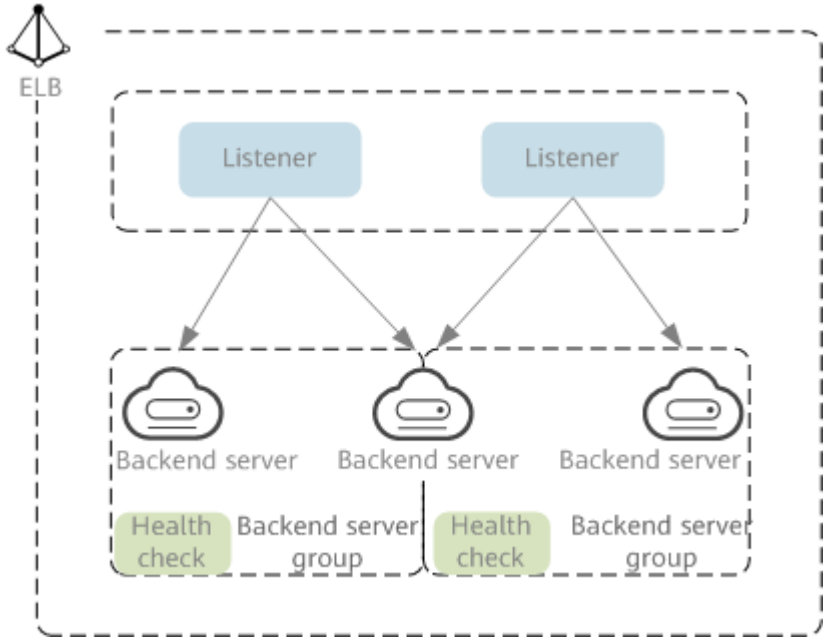
  

# 1 Balanceador de carga

## 1.1 Descripción general

Un balanceador de carga distribuye el tráfico entrante entre varios servidores backend. Antes de usar un balanceador de carga, debe agregar al menos un oyente y asociar un servidor backend con él.

**Figura 1-1** Componentes de ELB




### Tipo de red

Los balanceadores de carga pueden funcionar tanto en las redes públicas como en las privadas.

- Los balanceadores de carga en las solicitudes de ruta de red pública a través de Internet.

  Cada balanceador de carga tiene un EIP enlazado para que pueda recibir solicitudes de clientes en Internet y enrutar las solicitudes a través de servidores backend.

**Casos de aplicación:**

- Un balanceador de carga se utiliza como solo un punto de contacto para los clientes cuando un grupo de servidores proporciona servicios a través de Internet.
- La tolerancia a fallos y la recuperación de fallos son necesarias.

- Los balanceadores de carga en solicitudes de ruta de red privada dentro de una VPC.

  Este tipo de balanceadores de carga solo tiene direcciones IP privadas y se puede acceder solo en la VPC. Reciben solicitudes de clientes en una VPC y enrutan las solicitudes a través de servidores backend en la misma VPC.

  **Casos de aplicación:**

  Tanto los clientes como los servidores backend están en la misma VPC que el balanceador de carga.

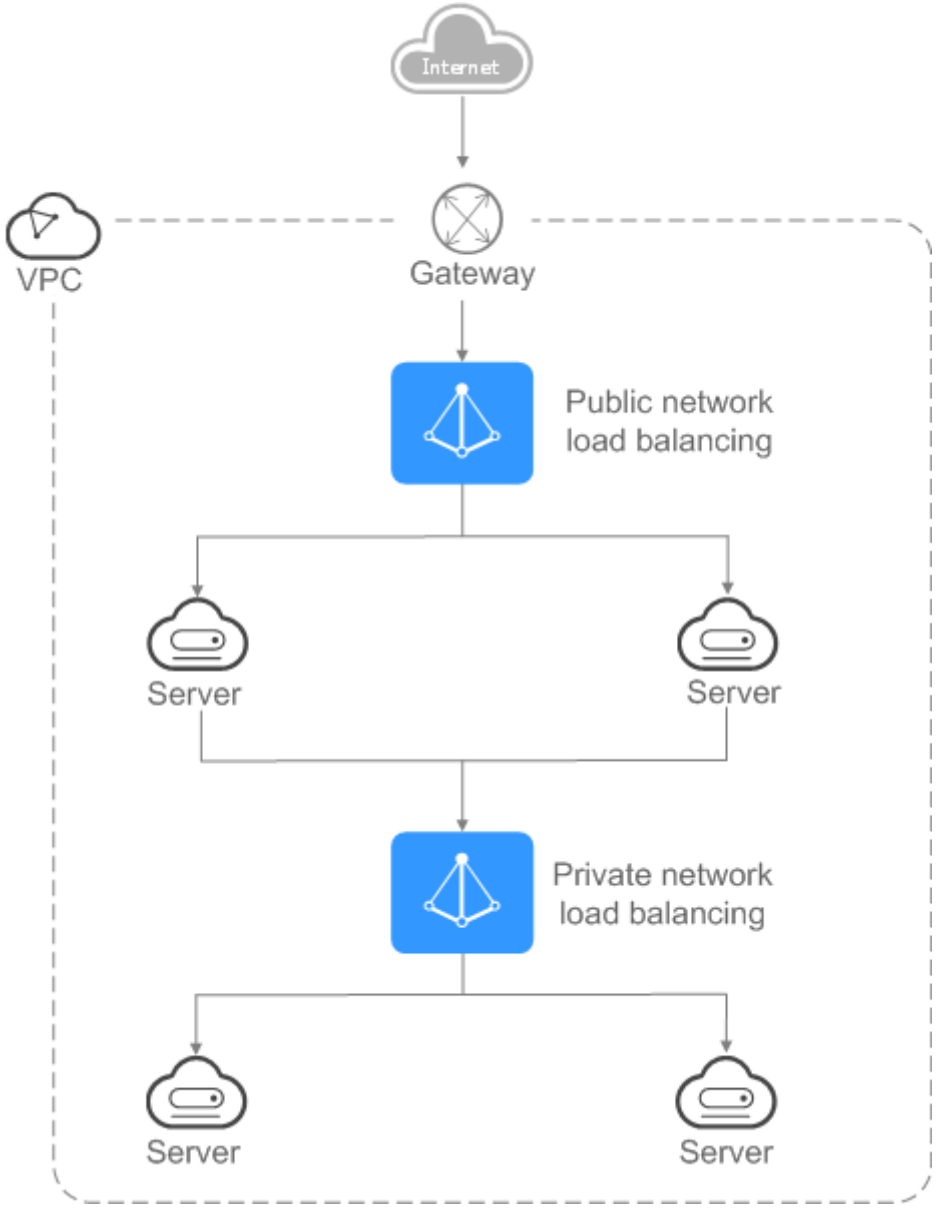
  - Hay varios servidores backend, y las solicitudes deben distribuirse uniformemente entre estos servidores.
  - La tolerancia a fallos y la recuperación de fallos son necesarias.
  - No desea que se expongan las direcciones IP de sus dispositivos físicos.

  **Los balanceadores de carga en las redes públicas y las privadas**

  Suponga que ha implementado servidores web y servidores de base de datos. Los servidores web son accesibles desde los usuarios en Internet, mientras que los servidores de base de datos solo se puede acceder a través de la red privada. En este caso, puede crear dos balanceadores de carga, uno para los servidores web y otro para los servidores de base de datos. El balanceador de carga en la red pública recibe solicitudes a través de Internet y enruta las solicitudes a los servidores web. A continuación, el balanceador de carga en la red privada reenvía las solicitudes a los servidores de base de datos.

**Figura 1-2** Los balanceadores de carga en las redes públicas y las privadas




# 1.2 Preparativos para crear un balanceador de carga

Antes de crear un balanceador de carga, debe planificar su región, red, protocolo y servidores backend.

## Región

Cuando seleccione una región, tenga en cuenta lo siguiente:

- La región debe estar cerca de los usuarios para reducir la latencia de la red y mejorar la velocidad de descarga.
- Los balanceadores de carga compartidos no pueden distribuir el tráfico entre regiones. Al crear el balanceador de carga, seleccione la misma región que los servidores backend.

- Puede asociar servidores backend entre regiones o en una VPC diferente con un balanceador de carga dedicado de cualquiera de las siguientes maneras:
  - Si los servidores de backend se encuentran en las diferentes VPC, puede usar Cloud Connect para conectar las VPC en todas las regiones. Para obtener más información, consulte la **Guía del usuario de Cloud Connect**.
  - Para agregar servidores backend en una VPC diferente o en un centro de datos local, debe habilitar **IP as a Backend** para el balanceador de carga. Para obtener más información, consulte la **Configuración de equilibrio de carga híbrido**.

## AZ

Los balanceadores de carga dedicados se pueden desplegar entre las AZ. Si selecciona varias AZ, se crea un balanceador de carga en cada AZ seleccionada.

Los balanceadores de carga en estas AZ funcionan en modo activo-activo o multiactivo para que las solicitudes sean distribuidas por el balanceador de carga más cercano en la misma AZ.

Seleccione la AZ donde residen los servidores backend para reducir la latencia de la red y mejorar la velocidad de acceso

Si se requiere recuperación ante desastres, cree balanceadores de carga basados en el escenario:

- **Un balanceador de carga en múltiples AZ (recuperación de desastres en el nivel de AZ)**

  Si el número de solicitudes no supera lo que pueden manejar las especificaciones más grandes (large II), puede crear un balanceador de carga y seleccionar varias AZ. De esta manera, si el balanceador de carga en una sola AZ es anormal, el balanceador de carga en otras AZ puede encaminar el tráfico, y la recuperación de desastres puede implementarse entre múltiples AZ.
- Múltiples balanceadores de carga y cada balanceador de carga en múltiples AZ (recuperación de desastres tanto en el balanceador de carga como en el nivel AZ)

  Si el número de solicitudes excede lo que pueden manejar las especificaciones más grandes (large II), puede crear varios balanceadores de carga y seleccionar varias AZ para cada balanceador de carga. De esta manera, si un solo balanceador de carga es anormal, otros balanceadores de carga pueden distribuir el tráfico, y la recuperación de desastres puede implementarse entre múltiples balanceadores de carga y AZ.

NOTA

- Si las solicitudes provienen de Internet, el balanceador de carga en cada AZ que seleccione encamina las solicitudes basadas en las direcciones IP de origen. Si desplegar un balanceador de carga en dos AZ, las solicitudes que los balanceadores de carga pueden manejar se duplicarán.
- Para solicitudes de una red privada:
  - Si los clientes están en la AZ seleccionada al crear el balanceador de carga, las solicitudes son distribuidas por el balanceador de carga en esta AZ. Si el balanceador de carga no está disponible, las solicitudes son distribuidas por el balanceador de carga en otra AZ seleccionada.

    Si el balanceador de carga está disponible pero las conexiones que el balanceador de carga necesita manejar exceden la cantidad definida en las especificaciones, el servicio puede interrumpirse. Para solucionar este problema, necesita actualizar las especificaciones. Puede monitorear el uso del tráfico en la red privada por AZ.
  - Si los clientes están en una AZ que no está seleccionada al crear el balanceador de carga, el balanceador de carga distribuye las solicitudes en cada AZ que seleccione en función de las direcciones IP de origen.
- Si las solicitudes provienen de una conexión de Direct Connect, el balanceador de carga de la misma AZ que la conexión de Direct Connect enruta las solicitudes. Si el balanceador de carga en esta AZ no está disponible, las solicitudes son distribuidas por el balanceador de carga en otra AZ.
- Si los clientes están en una VPC que es diferente de donde funciona el balanceador de carga, el balanceador de carga en la AZ donde reside la subred de VPC original enruta las solicitudes. Si el balanceador de carga en esta AZ no está disponible, las solicitudes son distribuidas por el balanceador de carga en otra AZ.

## Tipo de red

**Los balanceadores de carga dedicados admiten redes IPv4 públicas, redes IPv6 y redes IPv4 privadas.**

- Si selecciona la red IPv4 pública, el balanceador de carga tendrá un EIP IPv4 enlazado para enrutar las solicitudes a través de Internet.
- Si selecciona la red IPv4 privada, se asignará una dirección IPv4 privada al balanceador de carga para enrutar las solicitudes dentro de una VPC.
- Si selecciona la red IPv6, el balanceador de carga tendrá una dirección IPv6, que permite que el balanceador de carga enrute las solicitudes dentro de una VPC. Si agrega la dirección IPv6 a un ancho de banda compartido, el balanceador de carga también puede procesar solicitudes a través de Internet.

Los balanceadores de carga compartidos pueden funcionar tanto en redes públicas como privadas.

- Para enrutar solicitudes a través de Internet, debe vincular un EIP al balanceador de carga. El balanceador de carga también tiene una dirección IP privada y puede enrutar solicitudes en una VPC.
- Para enrutar solicitudes en una VPC, enlaza solo una dirección IP privada al balanceador de carga.

## Especificaciones

Los balanceadores de carga dedicados ofrecen una amplia gama de especificaciones para satisfacer sus requisitos en diferentes escenarios. Las especificaciones para el equilibrio de carga de red son adecuadas para solicitudes TCP o UDP, mientras que las especificaciones para el equilibrio de carga de aplicaciones se usan ampliamente para manejar solicitudes HTTP o HTTPS. Seleccione las especificaciones adecuadas según el volumen de tráfico y los

requisitos de servicio. Para obtener más información, consulte **Especificaciones de balanceadores de carga dedicados**.

Los siguientes son algunos principios para que usted seleccione las especificaciones:

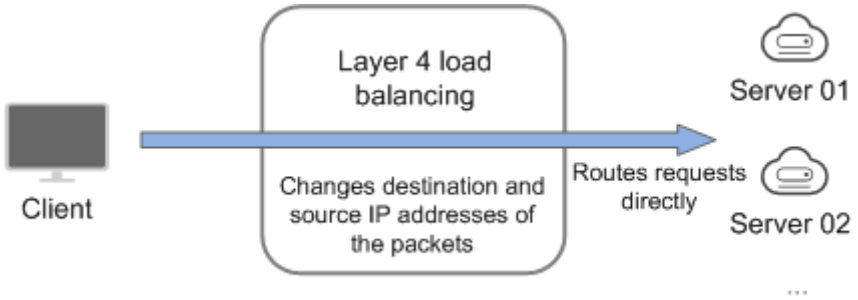
- Para el balanceo de carga TCP o UDP, preste atención al número de conexiones persistentes simultáneas y considere las conexiones simultáneas máximas como una métrica clave. Estime el número máximo de conexiones simultáneas que un balanceador de carga puede manejar en el escenario de servicio real y seleccione la especificación correspondiente.
- Para el balanceo de carga HTTP o HTTPS, concéntrese más en consultas por segundo (QPS), que determina el rendimiento del servicio de un sistema de aplicación. Estime el QPS que un balanceador de carga puede manejar en el escenario de servicio real y seleccionar la especificación correspondiente.
- Utilice los datos de monitorización de Cloud Eye para analizar el tráfico máximo, la tendencia y la regularidad del tráfico para seleccionar las especificaciones con mayor precisión.

## Protocolo

ELB ofrece equilibrio de carga tanto en capa 4 como en capa 7.

- Si elige TCP o UDP, el balanceador de carga se dirige directamente a los servidores backend. En este proceso, la dirección IP de destino en los paquetes se cambia a la dirección IP del servidor backend, y la dirección IP de origen a la dirección IP privada del balanceador de carga. Una conexión se establece después de un protocolo de enlace de tres vías entre el cliente y el servidor backend, y el balanceador de carga solo reenvía los datos.

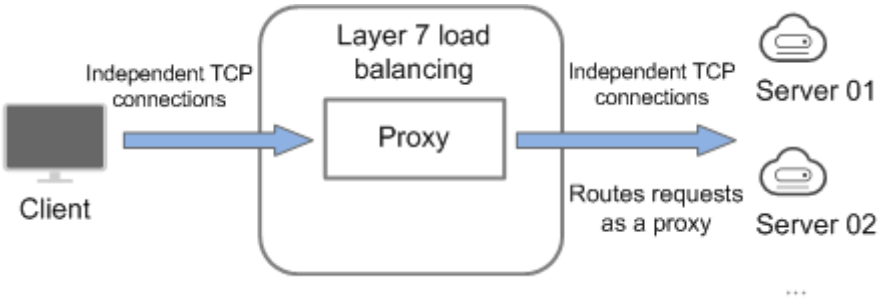
  **Figura 1-3** Balanceo de carga de capa 4




- El equilibrio de carga en la Capa 7 también se denomina "intercambio de contenido". Después de que el balanceador de carga recibe una solicitud, funciona como un proxy de servidores backend para establecer una conexión (hace de enlace de tres vías) con el cliente y luego determina a qué servidor backend se va a enrutar la solicitud basándose en los campos en la solicitud HTTP/HTTPS encabezado y el algoritmo de equilibrio de carga que seleccionó al agregar el oyente.

**Figura 1-4** Balanceo de carga de capa 7




### Servidores backend

Antes de usar ELB, debe crear servidores en la nube, desplegar las aplicaciones necesarias en ellos y agregar los servidores en la nube a uno o más grupos de servidores backend. Cuando cree ECS o BMS, tenga en cuenta lo siguiente:

- Los servidores en la nube deben estar en la misma región que el balanceador de carga.
- Se recomiendan los servidores en la nube que ejecuten el mismo SO para que pueda gestionarlos más fácilmente.

## 1.3 Creación de un balanceador de carga dedicado

### Escenarios

Ha preparado todo lo necesario para crear un balanceador de carga. Para obtener más información, véase **Preparativos para crear un balanceador de carga**.

### Restricciones

- Después de crear un balanceador de carga, la VPC no se puede cambiar. Si desea cambiar la VPC, cree un balanceador de carga y seleccione una VPC diferente.
- Para hacer ping a la dirección IP de un balanceador de carga, necesita agregar un oyente a él.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, haga clic en Compra de Elastic Load Balancer. Complete las configuraciones básicas basadas en **Tabla 1-1**.

**Tabla 1-1** Parámetros para configurar la información básica

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Type | Especifica el tipo del balanceador de carga. El tipo no se puede cambiar después de crear el balanceador de carga.<br>Para obtener más información sobre las diferencias, consulte **Diferencias entre los balanceadores de carga dedicados y compartidos**. | Dedicated |
| Billing Mode | Especifica el modo de facturación del balanceador de carga dedicado. Se le cobra por el tiempo que usa cada balanceador de carga. | Pay-per-use |
| Region | Especifica la región deseada. Los recursos en diferentes regiones no pueden comunicarse entre sí por las redes internas. Para una menor latencia de red y un acceso más rápido a los recursos, seleccione la región más cercana. | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| AZ | Especifica la AZ del balanceador de carga. Puede desplegar un balanceador de carga en varias AZ para obtener una alta disponibilidad. Si una AZ resulta defectuosa o no está disponible, los balanceadores de carga de otras AZ pueden enrutar solicitudes a servidores backend para garantizar la continuidad del servicio y mejorar la confiabilidad de las aplicaciones.<br>Si desplegar un balanceador de carga en varias AZ, su rendimiento, como el número de nuevas conexiones y el número de conexiones simultáneas se multiplicará. Por ejemplo, si despliega un balanceador de carga dedicado en dos AZ, puede manejar hasta 40 millones de conexiones simultáneas. | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| | **NOTA**<br>● Si las solicitudes provienen de Internet, el balanceador de carga en cada AZ que seleccione encamina las solicitudes basadas en las direcciones IP de origen. Si desplegar un balanceador de carga en dos AZ, las solicitudes que los balanceadores de carga pueden manejar se duplicarán.<br>● Para solicitudes de una red privada:<br>  ● Si los clientes están en la AZ seleccionada al crear el balanceador de carga, las solicitudes son distribuidas por el balanceador de carga en esta AZ. Si el balanceador de carga no está disponible, las solicitudes son distribuidas por el balanceador de carga en otra AZ seleccionada.<br>  Si el balanceador de carga está disponible pero las conexiones que el balanceador de carga necesita manejar exceden la cantidad definida en las especificaciones, el servicio puede interrumpirse. Para solucionar este problema, necesita actualizar las especificaciones. Puede monitorear el uso del tráfico en la red privada por AZ.<br>  ● Si los clientes están en una AZ que no está seleccionada al crear el balanceador de carga, el balanceador de carga distribuye las solicitudes en cada AZ que seleccione en función de las direcciones IP de origen.<br>● Si las solicitudes provienen de una conexión de Direct Connect, el balanceador de carga de la misma AZ que la conexión de Direct Connect enruta las solicitudes. Si el balanceador de carga en esta AZ no está disponible, las solicitudes son distribuidas por el balanceador de carga en otra AZ.<br>● Si los clientes están en una VPC que es diferente de donde funciona el balanceador de carga, el balanceador de carga en la AZ donde reside la subred de VPC original enruta las solicitudes. Si el balanceador de carga en esta AZ no está disponible, las solicitudes son distribuidas por el balanceador de carga en otra AZ. | |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Specifications | Seleccione **Elastic** o **Fixed** si se elige el modo de pago por uso como modo de facturación.<br>● Las especificaciones elásticas funcionan bien para el tráfico fluctuante, y se le cobrará por la cantidad de Load Balancer Capacity Unit (LCU, unidad de capacidad del balanceador de carga) que utiliza.<br>● Las especificaciones fijas son adecuadas para el tráfico estable, y se le cobrará por las especificaciones que seleccione.<br>Seleccione **Application load balancing (HTTP/HTTPS)** o **Network load balancing (TCP/UDP)** o ambos y, a continuación, seleccione la especificación deseada. Solo puede seleccionar una especificación para **Application load balancing (HTTP/HTTPS)** y **Network load balancing (TCP/UDP)**, respectivamente. Seleccione las especificaciones deseadas según el tamaño de su servicio consultando las **Especificaciones de balanceadores de carga dedicados**.<br>**NOTA**<br>Para obtener más información sobre las regiones en las que está disponible la especificación elástica, consulte **Descripción de funciones**. | Medium II |
| Name | Especifica el nombre del balanceador de carga. | elb-test |
| Enterprise Project | Especifica un proyecto de empresa mediante el cual los recursos de nube y los miembros se gestionan de forma centralizada. | default |
| Description | Proporciona información adicional sobre el balanceador de carga. | - |
| Tag | Identifica los balanceadores de carga para que se puedan encontrar fácilmente. Una etiqueta consiste en una clave de etiqueta y un valor de etiqueta.The tag key marks a tag, and the tag value specifies specific tag content. Para obtener más información sobre las especificaciones de nombres, consulte **Tabla 1-2**.<br>Se puede agregar un máximo de 10 etiquetas. | ● Key: elb_key1<br>● Value: elb-01 |

**Tabla 1-2** Reglas de nomenclatura de etiquetas

| Concepto | Requisito | Valor de ejemplo |
| --- | --- | --- |
| Clave de la etiqueta | ● Es un campo obligatorio.<br>● Debe ser único para el mismo balanceador de carga.<br>● Puede contener un máximo de 36 caracteres.<br>● Solo se permiten letras, dígitos, guiones bajos (_), guiones (-), arrobas (@) y caracteres chinos. | elb_key1 |
| Tag value | ● Puede contener un máximo de 43 caracteres.<br>● Solo se permiten letras, dígitos, guiones bajos (_), guiones (-), arrobas (@) y caracteres chinos. | elb-01 |

5. Configurar los parámetros de red basados en **Tabla 1-3**.

**Tabla 1-3** Parámetros para configuraciones de red

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| IP as a Backend | Especifica si se asocian los servidores backend que no están en la VPC del balanceador de carga. Una vez habilitada esta función, puede asociar los servidores backend con el balanceador de carga mediante sus direcciones IP.<br>**NOTA**<br>● Para utilizar esta función, configure las rutas de VPC correctas para garantizar que las solicitudes se puedan enrutar a los servidores backend.<br>● Si habilita esta función, se ocuparán más direcciones IP en la subred. Asegúrese de que la subred seleccionada tiene suficientes direcciones IP. Después de seleccionar una subred, puede ver el número de direcciones IP requeridas por el balanceador de carga en la información. | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Network Type | Especifica la red en la que funciona el balanceador de carga. Puede seleccionar uno o más tipos de red.<br>● **Public IPv4 network**: El balanceador de carga enruta las solicitudes de los clientes a los servidores backend a través de Internet.<br>● **Private IPv4 network**: El balanceador de carga enruta las solicitudes de los clientes a los servidores backend de una VPC.<br>● **IPv6 network**: Se asignará una dirección IPv6 al balanceador de carga para enrutar las solicitudes de los clientes IPv6.<br>**NOTA**<br>Si no selecciona ninguna de las opciones, el balanceador de carga no podrá comunicarse con los clientes después de su creación. Cuando utilice ELB o pruebe la conectividad de red, asegúrese de que el balanceador de carga tenga una dirección IP pública o privada enlazada. | Public IPv4 network |
| VPC | Especifica la VPC donde funciona el balanceador de carga.<br>Seleccione una VPC existente o cree una nueva.<br>Para obtener más información acerca de VPC, consulte la ***Guía del usuario de Virtual Private Cloud***. | vpc-test |
| Frontend Subnet | Especifica la subred en la que funcionará el balanceador de carga.<br>El sistema asigna direcciones IP a balanceadores de carga para recibir solicitudes basadas en el tipo de red configurado.<br>● **IPv4 private network**: asigna direcciones privadas IPv4.<br>● **IPv6 network**: asigna direcciones IPv6 privadas o públicas.<br>**NOTA**<br>Si selecciona **IPv6 network** para **Network Type** y la VPC seleccionada no tiene ninguna subred que admita IPv6, habilite IPv6 para las subredes o cree una subred que admita IPv6. Para obtener más información, consulte la **Guía del usuario de Virtual Private Cloud**. | subnet-test |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Subnet | El balanceador de carga utiliza las direcciones IP en la subred de backend para reenviar solicitudes a los servidores de backend.<br>● Seleccione **Subnet of the load balancer** de forma predeterminada.<br>● Seleccione una subred existente en la VPC donde funciona el balanceador de carga.<br>● Agregue una nueva subred<br>**NOTA**<br>● El número de direcciones IP requeridas depende de las especificaciones, el número de AZ y la IP como función de backend que haya configurado al crear el balanceador de carga. El número real de direcciones IP ocupadas depende del que se muestra en la consola.<br>● Un balanceador de carga de aplicaciones requiere de 8 a 30 direcciones IP adicionales en la subred de backend para el reenvío de tráfico. El número real de direcciones IP requeridas depende del tamaño del clúster de ELB. Si los balanceadores de carga se despliegan en el mismo clúster y funcionan en la misma subred backend, comparten las mismas direcciones IP para ahorrar recursos. | Subnet of the load balancer |
| Configuración de red IPv4 privada | | |
| IPv4 Address | Especifica cómo desea que se asigne la dirección IPv4.<br>● **Automatically assign IP address**: El sistema asigna automáticamente una dirección IPv4 al balanceador de carga.<br>● **Manually specify IP address**: Especificar manualmente una dirección IPv4 para el balanceador de carga.<br>**NOTA**<br>Las reglas de ACL de red configuradas para la subred de fondo del balanceador de carga no restringirán el tráfico de los clientes al balanceador de carga. Si se configuran las reglas de ACL de red, los clientes pueden acceder directamente al balanceador de carga. Para controlar el acceso al balanceador de carga, configure el control de acceso para todos los oyentes agregados al balanceador de carga.<br>Para obtener más información, véase **Control de acceso**. | Automatically assign IP address |
| Configuración de red IPv6 | | |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| IPv6 Address | Especifica cómo desea que se asigne la dirección IPv6.<br>**NOTA**<br>Las reglas de ACL de red configuradas para la subred de fondo del balanceador de carga no restringirán el tráfico de los clientes al balanceador de carga. Si se configuran las reglas de ACL de red, los clientes pueden acceder directamente al balanceador de carga. Para controlar el acceso al balanceador de carga, configure el control de acceso para todos los oyentes agregados al balanceador de carga.<br>Para obtener más información, véase **Control de acceso**. | Automatically assign IP address |
| Shared Bandwidth | Especifica el ancho de banda compartido al que se agregará la dirección IPv6.<br>Puede elegir no seleccionar un ancho de banda compartido, seleccionar un ancho de banda compartido existente o asignar un ancho de banda compartido. | Skip |
| Configuración de red IPv4 pública | | |
| EIP | Este parámetro es obligatorio cuando **Network Type** se establece en **IPv4 public network**.<br>● **New EIP**: El sistema asignará un nuevo EIP al balanceador de carga.<br>● **Use existing**: Seleccione una dirección IP existente. | - |
| EIP Type | Especifica el tipo de enlace (BGP) cuando se utiliza una nueva EIP.<br>**Dynamic BGP**: cuando se producen cambios en una red utilizando BGP dinámico, los protocolos de enrutamiento proporcionan una optimización automática en tiempo real de las configuraciones de red, lo que garantiza la estabilidad de la red y una experiencia óptima del usuario. | Dynamic BGP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Billed By | Especifica cómo se facturará el ancho de banda.<br>Puede seleccionar **Bandwidth**, **Traffic** o **Shared bandwidth**.<br>● **Bandwidth**: especifica el ancho de banda máximo y paga por la cantidad de tiempo que usa el ancho de banda.<br>● **Traffic**: especifica un ancho de banda máximo y paga por el tráfico saliente que usa.<br>● **Shared Bandwidth** | Shared Bandwidth |
| Bandwidth | Especifica el ancho de banda máximo. | 100 Mbit/s |

6. Haga clic en **Next**.
7. Confirme la configuración y envíe su solicitud.

# 1.4 Creación de un balanceador de carga compartido

## Escenarios

Ha preparado todo lo necesario para crear un balanceador de carga. Para obtener más información, véase **Preparativos para crear un balanceador de carga**.

Los balanceadores de carga reciben solicitudes de clientes y las enrutan a servidores backend, que responden a estas solicitudes a través de la red privada.

## Restricciones

- Después de crear un balanceador de carga, la VPC no se puede cambiar. Si desea cambiar la VPC, cree un balanceador de carga y seleccione una VPC diferente.
- Para hacer ping a la dirección IP de un balanceador de carga, necesita agregar un oyente y asociar un servidor backend a él.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Hover on in the upper left corner to display **Service List** and choose **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, haga clic en **Buy Elastic Load Balancer**. Configure los parámetros basados en **Tabla 1-4**.

**Tabla 1-4** Parámetros para configurar la información básica

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Type | Especifica el tipo del balanceador de carga. El tipo no se puede cambiar después de crear el balanceador de carga.<br>Para obtener más información sobre las diferencias, consulte **Diferencias entre los balanceadores de carga dedicados y compartidos**. | Shared |
| Billing Mode | Especifica el modo de facturación del balanceador de carga compartido. Se le cobra por el tiempo que usa cada balanceador de carga. | Pay-per-use |
| Region | Especifica la región deseada. Los recursos en diferentes regiones no pueden comunicarse entre sí por las redes internas. Para una menor latencia de red y un acceso más rápido a los recursos, seleccione la región más cercana. | - |
| Name | Especifica el nombre del balanceador de carga. | elb-test |
| Enterprise Project | Especifica un proyecto de empresa mediante el cual los recursos de nube y los miembros se gestionan de forma centralizada. | default |
| Description | Proporciona información adicional sobre el balanceador de carga. | - |
| Tag | Identifica los balanceadores de carga para que se puedan encontrar fácilmente. Una etiqueta consiste en una clave de etiqueta y un valor de etiqueta. La clave de etiqueta marca una etiqueta y el valor de etiqueta especifica contenido de etiqueta específico. Para obtener más información sobre las especificaciones de nombres, consulte **Tabla 1-5**.<br>Se puede agregar un máximo de 10 etiquetas. | ● Key: elb_key1<br>● Value: elb-01 |

**Tabla 1-5** Reglas de nomenclatura de etiquetas

| Concepto | Requisito | Valor de ejemplo |
|---|---|---|
| Clave de la etiqueta | ● Es un campo obligatorio.<br>● Debe ser único para el mismo balanceador de carga.<br>● Puede contener un máximo de 36 caracteres.<br>● Solo se permiten letras, dígitos, guiones bajos (_), guiones (-), arrobas (@) y caracteres chinos. | elb_key1 |
| Tag value | ● Puede contener un máximo de 43 caracteres.<br>● Solo se permiten letras, dígitos, guiones bajos (_), guiones (-), arrobas (@) y caracteres chinos. | elb-01 |

5. Configurar los parámetros de red basados en **Tabla 1-6**.

**Tabla 1-6** Parámetros para configuraciones de red

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Network Type | Especifica el tipo de red de un balanceador de carga. Puede seleccionar cualquiera de las siguientes opciones:<br>● **Public network**: El balanceador de carga enruta las solicitudes de los clientes a los servidores backend a través de Internet.<br>● **Private network**: Un balanceador de carga de red privada enruta las solicitudes de los clientes a los servidores backend en la misma VPC. | Public IPv4 network |
| VPC | Especifica la VPC donde funcionará el balanceador de carga.<br>Seleccione una VPC existente o cree una nueva.<br>Para obtener más información acerca de VPC, consulte la ***Guía del usuario de Virtual Private Cloud***. | - |
| Frontend Subnet | Especifica la subred en la que funcionará el balanceador de carga. Los balanceadores de carga compartidos admiten la red IPv4 privada de forma predeterminada.<br>El sistema asigna direcciones privadas IPv4 en esta subred a balanceadores de carga. | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| IPv4 Address | Especifica cómo desea que se asigne la dirección IPv4.<br>● **Automatically assign IP address**: El sistema asigna automáticamente una dirección IPv4 al balanceador de carga.<br>● **Manually specify IP address**: Especificar manualmente una dirección IPv4 para el balanceador de carga.<br>**NOTA**<br>Las reglas de ACL de red configuradas para la subred de fondo del balanceador de carga no restringirán el tráfico de los clientes al balanceador de carga. Si se configuran las reglas de ACL de red, los clientes pueden acceder directamente al balanceador de carga. Para controlar el acceso al balanceador de carga, configure el control de acceso para todos los oyentes agregados al balanceador de carga.<br>Para obtener más información, véase **Control de acceso**. | Automatically assign IP address |
| Guaranteed Performance | Especifica si se activa la opción de rendimiento garantizado. Esta función permite a sus balanceadores de carga manejar hasta 50,000 conexiones simultáneas, 5,000 nuevas conexiones por segundo y 5,000 consultas por segundo.<br>Esta función está habilitada de forma predeterminada y no se puede deshabilitar. | - |
| EIP | Especifica la dirección IP pública que estará enlazada al balanceador de carga para recibir y reenviar solicitudes a través de Internet.<br>Puede utilizar un EIP existente o solicitar uno nuevo.<br>Las siguientes opciones están disponibles:<br>● **New EIP**: El sistema asignará automáticamente una EIP.<br>● **Use existing**: Seleccione una EIP existente. | New EIP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| EIP Type | Especifica el tipo de enlace (BGP) cuando se utiliza una nueva EIP.<br>● **Static BGP**: cuando se producen cambios en una red que utiliza BGP estático, los operadores no pueden ajustar las configuraciones de red en tiempo real para garantizar una experiencia de usuario óptima.<br>● **Dynamic BGP**: cuando se producen cambios en una red utilizando BGP dinámico, los protocolos de enrutamiento proporcionan una optimización automática en tiempo real de las configuraciones de red, lo que garantiza la estabilidad de la red y una experiencia óptima del usuario. | Dynamic BGP |
| Billed By | Especifica cómo se facturará el ancho de banda.<br>Puede seleccionar cualquiera de las siguientes opciones:<br>● **Bandwidth**: especifica el ancho de banda máximo y paga por la cantidad de tiempo que usa el ancho de banda.<br>● **Traffic**: Usted especifica un ancho de banda máximo y paga por el tráfico total que usa.<br>**NOTA**<br>● Una EIP anual/mensual se cobra por ancho de banda fijo.<br>● Las EIP anuales/mensuales se pagan por adelantado. Las EIP anuales/mensuales no están disponibles para que elija cuando cree un balanceador de carga compartido. Puede asignar una EIP anual/mensual en la consola de EIP y seleccionarlo cuando cree el balanceador de carga. También puede vincular una EIP anual/mensual a un balanceador de carga existente. | Bandwidth |
| Bandwidth | Especifica el ancho de banda máximo cuando se utiliza una nueva EIP, en Mbit/s. | 10 Mbit/s |

6. Haga clic en **Next**.
7. Confirme la configuración y envíe su solicitud.

# 1.5 Habilitación del rendimiento garantizado para un balanceador de carga compartido

## Escenarios

El rendimiento garantizado permite a los balanceadores de carga compartidos manejar hasta 50,000 conexiones simultáneas, 5,000 nuevas conexiones por segundo y 5,000 consultas por segundo. Le proporciona capacidades de balanceo de carga más estables y confiables en caso de aumento de tráfico.

Si sus balanceadores de carga compartidos se crearon después del 10 de febrero de 2023, el rendimiento garantizado se habilitó para ellos de forma predeterminada.

Si los balanceadores de carga compartidos se crearon antes del 10 de febrero de 2023, realice las siguientes operaciones para habilitar el rendimiento garantizado.

## Notas

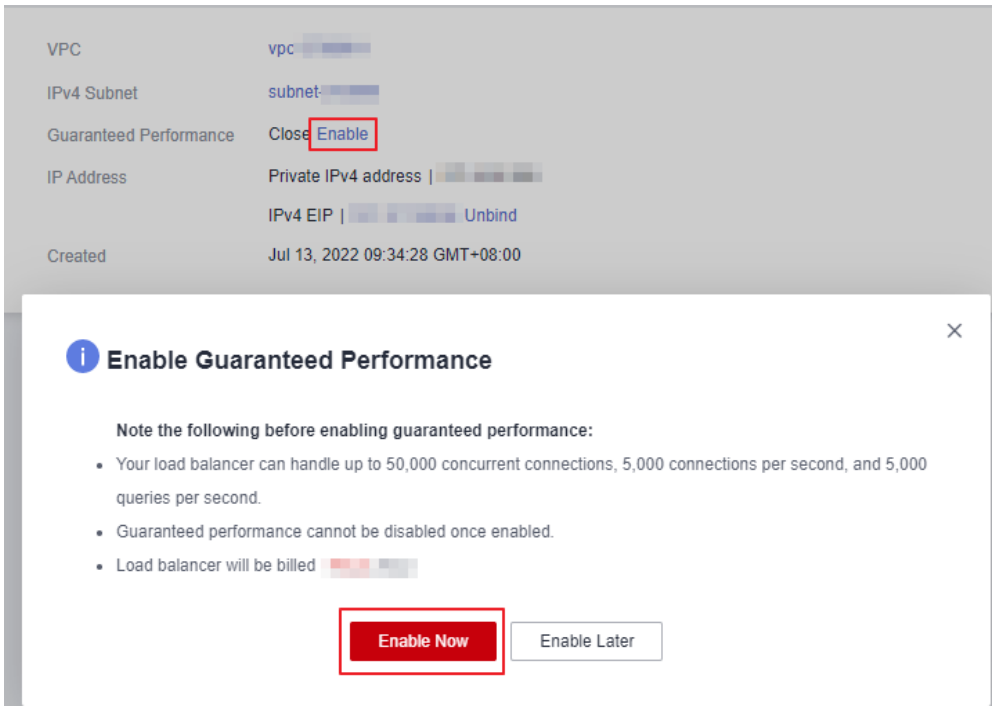
- El rendimiento garantizado no se puede deshabilitar una vez habilitado.
- Después de habilitar el rendimiento garantizado, los balanceadores de carga compartidos se cobrarán según el pago por uso. Para obtener más información sobre los precios de los productos, consulte **Detalles de precios de los productos**.

## Habilitación del rendimiento garantizado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Haga clic en el balanceador de carga compartido de destino para entrar en la página **Summary**.
5. Haga clic en **Enable**.
6. Haga clic en **Enable Now** para habilitar el rendimiento garantizado.

**Figura 1-5** Habilitación del rendimiento garantizado




# 1.6 Configuración de la protección de modificación para balanceadores de carga

## Escenario

Puede habilitar la protección de modificación para los balanceadores de carga para evitar que se modifiquen o eliminen por accidente.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En la página de la ficha **Summary**, haga clic en **Configure** junto a **Modification Protection**.
6. En el cuadro de diálogo **Configure Modification Protection**, habilite **Modification Protection**.

   Rellene el motivo si es necesario.
7. Haga clic en **OK**.

NOTA

Deshabilite **Modification Protection** si desea modificar o eliminar un balanceador de carga.

# 1.7 Modificación del ancho de banda

## Escenario

Si establece el **Network Type** de un balanceador de carga en **Public IPv4 network** o **IPv6 network**, el balanceador de carga puede enrutar solicitudes a través de Internet y puede modificar el ancho de banda utilizado por la EIP vinculada al balanceador de carga según sea necesario.

NOTA

- Al cambiar el ancho de banda, debe cambiar las especificaciones del balanceador de carga dedicado para evitar el límite de velocidad debido a un ancho de banda insuficiente.
- El ancho de banda de la EIP unida al balanceador de carga es el límite para el tráfico requerido por los clientes para acceder al balanceador de carga.

## Modificación del ancho de banda

Cuando se modifica el ancho de banda, el enrutamiento del tráfico no se interrumpirá.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en **More** en la columna **Operation**.
5. Balanceadores de carga dedicados: haga clic en **Modify IPv4 Bandwidth** o **Modify IPv6 Bandwidth**.

   Balanceadores de carga compartidos: haga clic en **Modify IPv4 Bandwidth**.
6. En el área **New Configuration**, modifique la opción de facturación y ancho de banda y haga clic en **Next**.

   Puede seleccionar el ancho de banda definido por el sistema o personalizar el ancho de banda. El ancho de banda varía de 1 Mbit/s a 2,000 Mbit/s.
7. Confirme el ancho de banda modificado y haga clic en **Pay Now**.

   NOTA

   Después de cambiar la opción de facturación y el ancho de banda, el precio se volverá a calcular en consecuencia.

# 1.8 Cambio de las especificaciones de un balanceador de carga dedicado

## Escenario

Puede cambiar las especificaciones de un balanceador de carga dedicado en la consola:

- Cambie un balanceador de carga de aplicación a un balanceador de carga de red, o al revés.
- Actualizar o degradar las especificaciones, por ejemplo, actualizar pequeño I a medio I, o degradar grande I a medio I.

NOTA

Solo puede cambiar las especificaciones de los balanceadores de carga dedicados.

## Cambio de especificaciones

**Tabla 1-7** Cambio de las especificaciones

| Tipo de balanceo de carga | Adición de tipo de balanceo de carga | Eliminación del tipo de balanceo de carga | Actualización de especificaciones | Degradación de especificaciones | Descripción |
|---|---|---|---|---|---|
| Balanceo de carga de red (TCP/UDP) | √ | √ | √ | √ | Si selecciona el balanceo de carga de red (TCP/UDP), solo puede crear un oyente TCP o UDP. |
| Balanceo de carga de aplicaciones (HTTP/HTTPS) | √ | √ | √ | √ | Si selecciona el balanceo de carga de la aplicación (HTTP/HTTPS), solo puede crear un oyente HTTP o HTTPS. |

ATENCIÓN

Los tipos y especificaciones de balanceo de carga disponibles pueden variar dependiendo de las diferentes regiones.

NOTA

La reducción de las especificaciones afectará temporalmente a los servicios.

- Balanceo de carga de red (TCP/UDP): es posible que no se establezcan nuevas conexiones.
- Balanceo de carga de aplicaciones (HTTP/HTTPS): Es posible que no se puedan establecer nuevas conexiones y que algunas conexiones persistentes se interrumpan.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga cuyas especificaciones desea modificar, haga clic en **More** en la columna **Operation** y seleccione **Change Specifications**.
5. Seleccione las nuevas especificaciones y haga clic en **Next**.
6. Confirme la información y haga clic en **Submit**.

# 1.9 Cambio del modo de facturación o de la opción de facturación de ancho de banda

## Cambio de la opción de facturación de ancho de banda

**Escenarios**

Para los balanceadores de carga de red pública, puede cambiar sus opciones de facturación (facturadas por ancho de banda o tráfico) según sea necesario.

Después de cambiar la opción de facturación, el precio se volverá a calcular en consecuencia.

**Procedimiento**

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el área **New Configuration**, cambie la opción de facturación y haga clic en **Next**.
5. Confirme la nueva opción de facturación y haga clic en **Submit**.

# 1.10 Cambio de una dirección IP

## Escenarios

Puede cambiar la dirección IPv4 privada y la dirección IPv6 enlazada a un balanceador de carga.

- Puede cambiar la dirección IPv4 privada a otra dirección IP IPv4 en la subred actual u otras subredes.
- Puede cambiar la dirección IPv6 a otra dirección IP IPv6 en otras subredes.

Puede cambiar la dirección IPv4 privada enlazada a un balanceador de carga a otra dirección IP IPv4 en la subred actual u otras subredes.

NOTA

Solo puede cambiar la dirección IP vinculada a un balanceador de carga dedicado.

## Restricciones

Para cambiar la dirección IPv6, asegúrese de que la VPC donde funciona el balanceador de carga tenga subredes con IPv6 habilitado.

## Cambio de una dirección IPv4 privada

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga cuya dirección IP desea cambiar y haga clic en **More** > **Change Private IPv4 Address** en la columna **Operation**.
5. En el cuadro de diálogo **Change Private IPv4 Address**, seleccione la subred donde reside la dirección IP y especifique la dirección IP.
   - Para utilizar una dirección IP de otra subred, seleccione **Automatically assign IPv4 address**. El sistema asigna automáticamente una dirección IPv4 para el balanceador de carga.
   - Para utilizar otra dirección IP de la subred actual, especifique una dirección IP.
6. Haga clic en **OK**.

## Cambio de una dirección IPv6

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga cuya dirección IP desea cambiar y haga clic en **More** > **Change IPv6 Address** en la columna **Operation**.
5. En el cuadro de diálogo **Change IPv6 Address**, seleccione una subred diferente donde reside la dirección IP y especifique la dirección IP.

   El sistema asignará automáticamente una dirección IPv6 al balanceador de carga desde la subred que seleccione.

6. Haga clic en **OK**.

# 1.11 Vinculación de una dirección IP a o desvinculación de una dirección IP de un balanceador de carga

## Escenarios

Puede vincular una dirección IP a un balanceador de carga o desvincular la dirección IP de un balanceador de carga según los requisitos del servicio.

- Una dirección IPv6, una EIP IPv4 y una dirección IPv4 privada pueden estar enlazadas o no enlazadas de un balanceador de carga dedicado.
- Solo una EIP IPv4 puede estar enlazada a o desvinculada de un balanceador de carga compartido.

NOTA

- Los balanceadores de carga sin IPv4 EIP no pueden enrutar solicitudes a través de la red IPv4 pública.
- Los balanceadores de carga sin direcciones IPv4 privadas no pueden enrutar solicitudes por la red IPv4 privada.
- Una vez que una dirección IPv6 no está enlazada, el balanceador de carga no puede enrutar solicitudes a través de la red IPv6.

## Vinculación de una EIP IPv4

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga al que desea enlazar una EIP IPv4 y haga clic en **More** > **Bind IPv4 EIP** en la columna **Operation**.
5. En el cuadro de diálogo **Bind IPv4 EIP**, seleccione el EIP que desea vincular al balanceador de carga.
6. Haga clic en **OK**.

## Vinculación de una dirección IPv4 privada

Solo los balanceadores de carga dedicados admiten esta función.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.

4. En la página **Load Balancers**, busque el balanceador de carga al que desea enlazar una dirección IPv4 privada y haga clic en **More** > **Bind Private IPv4 Address** en la columna **Operation**.
5. En el cuadro de diálogo **Bind Private IPv4 Address**, seleccione la subred donde reside la dirección IP y especifique la dirección IP.
   - De forma predeterminada, el sistema asigna automáticamente una dirección IP. Para especificar manualmente una dirección IP, anule la selección de **Automatically assign IP address** e introduzca la dirección IP.
   - Asegúrese de que la dirección IP introducida pertenece a la subred seleccionada y no está en uso.
6. Haga clic en **OK**.

## Vinculación de una dirección IPv6

Solo los balanceadores de carga dedicados pueden tener direcciones IPv6 enlazadas.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página de la ficha **Elastic Load Balancers**, busque el balanceador de carga al que desea enlazar una dirección IPv6 y haga clic en **More** > **Bind IPv6 Address** en la columna **Operation**.
5. En el cuadro de diálogo **Bind IPv6 Address**, seleccione la subred donde reside la dirección IP.
6. Haga clic en **OK**.

## Desvinculación de un EIP IPv4

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga del que desea desvincular el EIP IPv4 y haga clic en **More** > **Unbind IPv4 EIP** en la columna **Operation**.
5. En el cuadro de diálogo que se muestra, confirme la EIP IPv4 que desea desvincular y haga clic en **Yes**.

   NOTA

   Después de que el IPv4 EIP no está enlazado, el balanceador de carga no puede enrutar solicitudes a través de Internet.

## Desvinculación de una dirección IPv4 privada

Solo los balanceadores de carga dedicados admiten esta función.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga del que desea desvincular la dirección IPv4 privada y haga clic en **More** > **Unbind Private IPv4 Address** en la columna **Operation**.
5. En el cuadro de diálogo que se muestra, confirme la dirección IPv4 privada que desea desvincular y haga clic en **Yes**.

   NOTA

   Una vez que la dirección IPv4 privada no está enlazada, el balanceador de carga no puede enrutar solicitudes a través de la red IPv4 privada.

### Desvinculación de una dirección IPv6

Solo los balanceadores de carga dedicados pueden tener direcciones IPv6 enlazadas.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga del que desea desvincular la dirección IPv6 y haga clic en **More** > **Unbind IPv6 Address** en la columna **Operation**.
5. En el cuadro de diálogo que se muestra, confirme la dirección IPv6 que desea desvincular y haga clic en **Yes**.

   NOTA

   Una vez que una dirección IPv6 no está enlazada, el balanceador de carga no puede enrutar solicitudes a través de la red IPv6.

## 1.12 Adición o extracción de un ancho de banda compartido IPv6

### Escenarios

Después de vincular una dirección IPv6 a un balanceador de carga dedicado, puede agregar el balanceador de carga a un ancho de banda compartido para permitirle enrutar solicitudes por Internet. Una vez que haya terminado con el ancho de banda compartido, puede quitar el balanceador de carga del ancho de banda compartido, de modo que solo pueda enrutar solicitudes dentro de una VPC.

### Adición a un ancho de banda compartido IPv6

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga que desea agregar a un ancho de banda compartido y haga clic en **More** > **Add to IPv6 Shared Bandwidth** en la columna **Operation**.
5. En el cuadro de diálogo **Add to IPv6 Shared Bandwidth**, seleccione el ancho de banda compartido al que desea agregar el balanceador de carga dedicado.

   Si no hay anchos de banda compartidos disponibles, compre uno como se le indique.
6. Haga clic en **OK**.

### Eliminación de un ancho de banda compartido IPv6

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga que desea quitar de un ancho de banda compartido y haga clic en **More** > **Remove from IPv6 Shared Bandwidth** en la columna **Operation**.
5. En el cuadro de diálogo que se muestra, confirme el ancho de banda compartido que desea quitar.

   NOTA

   Después de eliminar el ancho de banda compartido, el balanceador de carga no puede enrutar solicitudes por Internet.
6. Haga clic en **Yes**.

## 1.13 Exportación de la lista de balanceadores de carga

### Escenarios

Puede exportar la lista del balanceador de carga para la copia de seguridad.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la esquina superior izquierda de la lista de balanceadores de carga, haga clic en **Export**.

# 1.14 Eliminación de un balanceador de carga

## Escenarios

Puede eliminar un balanceador de carga si ya no lo necesita.

**ATENCIÓN**

Los balanceadores de carga eliminados no se pueden recuperar.

Después de eliminar un balanceador de carga de red pública, su EIP no se liberará y puede ser utilizado por otros recursos.

## Requisitos previos

Elimine los recursos configurados para el balanceador de carga en la siguiente secuencia:

1. Elimine todas las políticas de reenvío agregadas a los oyentes HTTP y HTTPS del balanceador de carga.
2. Elimine la redirección creada para cada oyente HTTP del balanceador de carga.
3. Quite todos los servidores backend de los grupos de servidores backend asociados con cada oyente del balanceador de carga.
4. Elimine todos los oyentes agregados al balanceador de carga.
5. Elimine todos los grupos de servidores backend asociados con cada oyente del balanceador de carga.

## Eliminación de un balanceador de carga

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en **Delete** en la columna **Operation**.
5. Haga clic en **Yes**.

# 2 Oyente

## 2.1 Descripción general

Necesita agregar al menos un oyente después de haber creado un balanceador de carga. Este oyente recibe solicitudes de clientes y enruta solicitudes a los servidores backend utilizando el protocolo, el puerto y el algoritmo de balanceo de carga que seleccione.

### Protocolos soportados

ELB ofrece equilibrio de carga tanto en capa 4 como en capa 7.

Seleccione TCP o UDP para el equilibrio de carga en la capa 4 y HTTP o HTTPS en la capa 7.

**Tabla 2-1** Protocolos soportados por ELB

| Protocolo | | Descripción | Casos de aplicación: |
|---|---|---|---|
| Capa 4 | TCP | ● Sesiones adhesivas basadas en direcciones IP de origen<br>● Transferencia rápida de datos | ● Escenarios que requieren alta confiabilidad y precisión de los datos, como la transferencia de archivos, el correo electrónico y el inicio de sesión remoto<br>● Aplicaciones web que reciben un gran número de solicitudes simultáneas y requieren un alto rendimiento |
| Capa 4 | UDP | ● Baja confiabilidad<br>● Transferencia rápida de datos | Escenarios que requieren una respuesta rápida, como videochat, juegos y cotizaciones financieras en tiempo real |

| Protocolo | | Descripción | Casos de aplicación: |
|---|---|---|---|
| Capa 7 | HTTP | ● Sesiones adhesivas basadas en cookies<br>● Encabezado de solicitud X-Forward-For | Aplicaciones web en las que es necesario identificar el contenido de datos, como los juegos para móviles |
| Capa 7 | HTTPS | ● Una extensión de HTTP para la transmisión de datos cifrados para evitar el acceso no autorizado<br>● Cifrado y descifrado realizado en balanceadores de carga<br>● Múltiples versiones de protocolos de encriptación y conjuntos de encriptación | Aplicaciones web que requieren transmisión cifrada |

# 2.2 Protocolos y puertos

## Protocolos y puertos frontend

Los protocolos y puertos frontend son utilizados por los balanceadores de carga para recibir solicitudes de clientes. Los balanceadores de carga usan TCP o UDP en la capa 4, y HTTP o HTTPS en la capa 7. Seleccione un protocolo y un puerto que mejor se adapte a sus necesidades.

NOTA

Los protocolos frontend seleccionados y los puertos introducidos no se pueden cambiar. Si quieres cambiarlos, crea otro oyente.

**Tabla 2-2** Protocolos y puertos frontend

| Protocol | Puerto |
| --- | --- |
| TCP | Hay algunas restricciones al seleccionar los protocolos y los números de puerto.<br>● Para cada balanceador de carga, UDP puede utilizar los mismos puertos que otros protocolos, pero estos otros protocolos deben tener puertos únicos. Por ejemplo, si tiene un oyente UDP que utiliza el puerto 88, puede agregar un oyente TCP, HTTP o HTTPS que también utilice el puerto 88. Sin embargo, si ya tiene un oyente HTTP que usa el puerto 443, no puede agregar un oyente HTTPS o TCP que use el mismo puerto.<br>● Los números de puerto del mismo protocolo deben ser únicos. Por ejemplo, si tiene un oyente TCP que utiliza el puerto 80, no puede agregar otro oyente TCP que utilice el mismo puerto.<br>El número de puerto se encuentra dentro del rango de 1 a 65535.<br>Los siguientes son algunos protocolos y números de puerto de uso común:<br>TCP/80<br>HTTPS/443 |
| UDP | |
| HTTP | |
| HTTPS | |

## Protocolos y puertos de backend

Los protocolos y puertos backend son utilizados por los servidores backend para recibir solicitudes de balanceadores de carga. Si los servidores Windows tienen Internet Information Services (IIS) instalados, el protocolo y el puerto de backend predeterminados son HTTP y 80.

**Tabla 2-3** Protocolos y puertos backend

| Protocolo | Puerto |
| --- | --- |
| TCP | Los servidores backend pueden utilizar los mismos puertos. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>Los siguientes son algunos protocolos y números de puerto de uso común:<br>TCP/80<br>HTTP/80<br>HTTPS/443 |
| UDP | |
| QUIC | |
| HTTP | |
| HTTPS | |

# 2.3 Adición de un oyente de TCP

## Escenarios

Puede agregar un oyente TCP, si se requiere alta confiabilidad y alta precisión, pero la velocidad lenta es aceptable, por ejemplo, durante la transferencia de archivos, envío y recepción de correo electrónico, e inicio de sesión remoto.

## Restricciones

- Si el protocolo oyente es TCP, el protocolo del grupo de servidores backend es TCP por defecto y no se puede cambiar.
- Si solo selecciona el balanceo de carga de aplicaciones (HTTP/HTTPS) para su balanceador de carga dedicado, no puede agregar un oyente de TCP a este balanceador de carga.

## Adición de un oyente de TCP a un balanceador de carga dedicado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configure los parámetros basados en **Tabla 2-4**.

**Tabla 2-4** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Name | Especifica el nombre de oyente. | listener-pnqy |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | TCP |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | Blacklist |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup-b2 |
| Transfer Client IP Address | Especifica si se deben transmitir las direcciones IP de los clientes a los servidores backend.<br>Esta función está habilitada para balanceadores de carga dedicados de forma predeterminada y no se puede deshabilitar. | N/A |
| **Configuración avanzada** | | |
| Idle Timeout | Especifica el período de tiempo que una conexión debe mantenerse activa, en segundos. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud.<br>La duración del tiempo de espera en reposo varía de **10** a **4000.** | 300 |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy** para configurar el grupo de servidores backend. Para obtener más información acerca de cómo configurar un grupo de servidores backend, consulte **Tabla 2-5**.

**Tabla 2-5** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend debe ser TCP. | Create new |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group |
| Backend Protocol | Especifica el protocolo utilizado por los servidores backend para recibir solicitudes.<br>El protocolo de backend es TCP por defecto y no se puede cambiar. | TCP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo utilizado por el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones activas establecidas con cada servidor backend, a cada servidor se le asigna una ponderación basada en su capacidad de procesamiento. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada se utiliza para asignar el cliente a un servidor en particular. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend.<br>Este parámetro es opcional si ha seleccionado **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas.<br>**Source IP address** es la única opción disponible cuando se utiliza TCP o UDP como protocolo frontend.<br>**Source IP address**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave de hash única, y todos los puntos de conexión se numeran. El sistema asigna el cliente a un punto de conexión particular basado en la clave generada. Las solicitudes de la misma dirección IP se reenvían al mismo servidor backend para su procesamiento. | Source IP address |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Description | Proporciona información adicional sobre el grupo de servidores backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para obtener los parámetros necesarios para configurar una comprobación de estado, consulte **Tabla 2-6**.

**Tabla 2-6** Parámetros para configurar una comprobación de estado

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada, haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend.<br>Si el protocolo de backend es TCP, el protocolo de comprobación de estado puede ser TCP, HTTP o HTTPS. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra inclinada (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras (/), puntos (.), signos de interrogación (?), signos numéricos (#), signos de porcentaje (%), ampersands (&) y conjuntos de caracteres extendidos _;~!.() *[]@$^:',+ | /index.html |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Especifica el tiempo máximo necesario para esperar una respuesta de la comprobación de estado, en segundos. La duración del tiempo de espera varía de **1** a **50**. | 3 |
| Maximum Retries | Especifica el número máximo de reintentos de comprobación de estado. El valor oscila entre **1** y **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

## Adición de un oyente de TCP a un balanceador de carga compartido

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configura los parámetros basados en **Tabla 2-7**.

**Tabla 2-7** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Name | Especifica el nombre de oyente. | listener-pnqy |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | TCP |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | Whitelist |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup-b2 |
| Transfer Client IP Address | Especifica si se deben transmitir las direcciones IP de los clientes a los servidores backend. Este parámetro está disponible cuando el protocolo oyente es TCP o UDP. | N/A |
| **Configuración avanzada** | | |
| Idle Timeout | Especifica el período de tiempo que una conexión debe mantenerse activa, en segundos. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud.<br>La duración del tiempo de espera en reposo varía de **10** a **4000**. | 300 |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy**. **Tabla 2-8** describe los parámetros para configurar un grupo de servidores backend.

**Tabla 2-8** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend debe ser TCP. | Create new |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group-sq4v |
| Backend Protocol | Especifica el protocolo utilizado por los servidores backend para recibir solicitudes.<br>El protocolo de backend es TCP por defecto y no se puede cambiar. | TCP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo utilizado por el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Este algoritmo está diseñado basado en el algoritmo de conexiones mínimas que utiliza el número de conexiones activas a cada servidor backend para tomar su decisión de balanceo de carga. Además del número de conexiones, a cada servidor se le asigna una ponderación basada en su capacidad. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada asigna el cliente a un servidor determinado. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend.<br>**NOTA**<br>Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas. **Source IP address** es la única opción disponible cuando se utiliza TCP o UDP como protocolo frontend.<br>**Source IP address**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave de hash única, y todos los puntos de conexión se numeran. El sistema asigna el cliente a un punto de conexión particular basado en la clave generada. Las solicitudes de la misma dirección IP se reenvían al mismo servidor backend para su procesamiento. | Source IP address |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Description | Proporciona información adicional sobre el grupo de servidores backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para ver los parámetros necesarios para configurar una comprobación de estado, consulte **Tabla 2-9**.

**Tabla 2-9** Parámetros para configurar una comprobación de estado

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada,<br>haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend. Hay dos opciones: TCP y HTTP. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra inclinada (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras diagonales (/), puntos (.), signos de interrogación (?), signos de porcentaje (%), ampersands (&) y guiones bajos (_). | /index.html |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Especifica el tiempo máximo necesario para esperar una respuesta de la comprobación de estado, en segundos. La duración del tiempo de espera varía de **1** a **50**. | 3 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Maximum Retries | Especifica el número máximo de reintentos de comprobación de estado. El valor oscila entre **1** y **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

# 2.4 Adición de un oyente de UDP

## Escenarios

Los oyentes de UDP son adecuados para escenarios que se centran más en la puntualidad que en la fiabilidad, como el chat de vídeo, los juegos y las cotizaciones en tiempo real en el mercado financiero.

## Restricciones

- Los oyentes de UDP no soportan la fragmentación.
- El puerto de los oyentes de UDP no puede ser 4789.
- Los paquetes de UDP pueden tener cualquier tamaño inferior a 1,500 bytes. Los paquetes serán descartados si son demasiado grandes. Es necesario modificar los archivos de configuración de las aplicaciones en función del valor máximo de la unidad de transmisión (MTU).
- Balanceadores de carga dedicados: El protocolo backend puede ser UDP o QUIC si el protocolo de oyente es UDP.
- Balanceadores de carga compartidos: Si el protocolo de oyente es UDP, el protocolo del grupo de servidores backend es UDP por defecto y no se puede cambiar.
- Si solo selecciona el balanceo de carga de aplicaciones (HTTP/HTTPS) para su balanceador de carga dedicado, no puede agregar un oyente de UDP a este balanceador de carga.

## Adición de un oyente de UDP a un balanceador de carga dedicado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configure los parámetros basados en **Tabla 2-10**.

**Tabla 2-10** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Name | Especifica el nombre de oyente. | listener |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | UDP |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | **Blacklist** |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup |
| Transfer Client IP Address | Especifica si se deben transmitir las direcciones IP de los clientes a los servidores backend.<br>Esta función está habilitada para balanceadores de carga dedicados de forma predeterminada y no se puede deshabilitar. | N/A |
| **Configuración avanzada** | | |
| Idle Timeout | Especifica el período de tiempo que una conexión debe mantenerse activa, en segundos. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud.<br>La duración del tiempo de espera en reposo varía de **10** a **4000**. | 300 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy** para configurar el grupo de servidores backend. **Tabla 2-11** describe los parámetros para configurar un grupo de servidores backend.

**Tabla 2-11** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend debe ser TCP. | Create new |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group |
| Backend Protocol | Especifica el protocolo que utilizarán los servidores backend para recibir solicitudes.<br>El protocolo de back-end puede ser UDP o QUIC. | UDP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo que utilizará el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones activas establecidas con cada servidor backend, a cada servidor se le asigna una ponderación basada en su capacidad de procesamiento. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada se utiliza para asignar el cliente a un servidor en particular. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend.<br>Este parámetro es opcional si ha seleccionado **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**. | N/A |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas. **Source IP address** es la única opción disponible cuando se utiliza TCP o UDP como protocolo frontend.<br>**Source IP address**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave de hash única, y todos los puntos de conexión se numeran. El sistema asigna el cliente a un punto de conexión particular basado en la clave generada. Las solicitudes de la misma dirección IP se reenvían al mismo servidor backend para su procesamiento. | Source IP address |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Description | Proporciona información adicional sobre el grupo de servidores backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para ver los parámetros necesarios para configurar una comprobación de estado, consulte **Tabla 2-12**.

**Tabla 2-12** Parámetros para configurar una comprobación de estado

| Parameter | Descripción | Example Value |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada, haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend.<br>Si el protocolo de backend es UDP, el protocolo de comprobación de estado es UDP y no se puede cambiar. | UDP |
| Health Check Port | Specifies the port that will be used by the load balancer to check the health of backend servers. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Specifies the maximum time required for waiting for a response from the health check, in seconds. The timeout duration ranges from **1** to **50**. | 3 |
| Maximum Retries | Specifies the maximum number of health check retries. The value ranges from **1** to **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

## Adición de un oyente de UDP a un balanceador de carga compartido

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.

3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configure los parámetros basados en **Tabla 2-13**.

**Tabla 2-13** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Name | Especifica el nombre de oyente. | listener |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | UDP |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | Whitelist |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup |
| Transfer Client IP Address | Especifica si se deben transmitir las direcciones IP de los clientes a los servidores backend. | N/A |
| **Configuración avanzada** | | |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy**. **Tabla 2-14** describe los parámetros para configurar un grupo de servidores backend.

**Tabla 2-14** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend debe ser TCP. | **Create new** |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group |
| Backend Protocol | Especifica el protocolo que utilizarán los servidores backend para recibir solicitudes.<br>El protocolo de backend es UDP por defecto y no se puede cambiar. | UDP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo utilizado por el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones activas establecidas con cada servidor backend, a cada servidor se le asigna una ponderación basada en su capacidad de procesamiento. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada se utiliza para asignar el cliente a un servidor en particular. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend.<br>**NOTA**<br>Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**. | N/A |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas. **Source IP address** es la única opción disponible cuando se utiliza TCP o UDP como protocolo frontend.<br>**Source IP address**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave de hash única, y todos los puntos de conexión se numeran. El sistema asigna el cliente a un punto de conexión particular basado en la clave generada. Las solicitudes de la misma dirección IP se reenvían al mismo servidor backend para su procesamiento. | Source IP address |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Description | Proporciona información adicional sobre el grupo de servidores backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para ver los parámetros necesarios para configurar una comprobación de estado, consulte **Tabla 2-15**.

**Tabla 2-15** Parámetros para configurar una comprobación de estado

| Parameter | Descripción | Example Value |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada, haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |
| Health Check Protocol | Specifies the protocol that will be used by the load balancer to check the health of backend servers. The health check protocol is UDP by default and cannot be changed. | UDP |
| Health Check Port | Specifies the port that will be used by the load balancer to check the health of backend servers. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Specifies the maximum time required for waiting for a response from the health check, in seconds. The timeout duration ranges from **1** to **50**. | 3 |
| Maximum Retries | Specifies the maximum number of health check retries. The value ranges from **1** to **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

# 2.5 Adición de un oyente de HTTP

## Escenarios

Los oyentes de HTTP son adecuados para aplicaciones que requieren identificar el contenido de datos, como aplicaciones web y pequeños juegos móviles.

## Restricciones

- Si el protocolo de oyente es HTTP, el protocolo del grupo de servidores backend es HTTP por defecto y no se puede cambiar.
- Si un balanceador de carga dedicado utiliza una especificación para el balanceo de carga de red (TCP/UDP), no puede crear un oyente de HTTP.

## Adición de un oyente de HTTP a un balanceador de carga dedicado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configure los parámetros basados en **Tabla 2-16**.

**Tabla 2-16** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Name | Especifica el nombre de oyente. | listener |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | HTTP |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |
| Redirect | Especifica si se va a habilitar la redirección.<br>Si tiene oyentes HTTPS y HTTP, puede usar esta función para redirigir las solicitudes desde el oyente HTTP al oyente HTTPS para garantizar la seguridad.<br>Si crea una redirección para un oyente HTTP, el servidor backend devolverá HTTP 301 Move Permanently a los clientes. | N/A |
| Redirected To | Especifica el oyente de HTTPS al que se redirigen las solicitudes si **Redirect** está habilitado. | listener_HTTPS_443 |

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | **Blacklist** |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup |
| Transfer Client IP Address | Especifica si se deben transmitir las direcciones IP de los clientes a los servidores backend.<br>Esta función está habilitada para balanceadores de carga dedicados de forma predeterminada y no se puede deshabilitar. | Enabled |
| Advanced Forwarding | Especifica si se debe habilitar la política de reenvío avanzado. Puede agregar políticas de reenvío avanzadas a oyentes HTTP o HTTPS para reenviar solicitudes a diferentes grupos de servidores backend según el método de solicitud HTTP, el encabezado HTTP, la cadena de consulta o el bloque CIDR, además de nombres de dominio y direcciones URL. | Enabled |
| **Configuración avanzada** | | |
| Idle Timeout | Especifica el período de tiempo que una conexión debe mantenerse activa, en segundos. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud.<br>La duración del tiempo de espera en reposo varía de **0** a **4000**. | 60 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Request Timeout | Especifica el período de tiempo (en segundos) después del cual el balanceador de carga cierra la conexión si el balanceador de carga no recibe una solicitud del cliente.<br>La duración del tiempo de espera de la solicitud varía de **1** a **300**. | 60 |
| Response Timeout | Especifica el período de tiempo (en segundos) después del cual el balanceador de carga envía un error de 504 Gateway Timeout al cliente si el balanceador de carga no recibe respuesta del servidor backend después de enrutar una solicitud al servidor backend y no recibe respuesta tras intentar enrutar la misma solicitud a otros servidores backend.<br>La duración del tiempo de espera de la respuesta varía de **1** a **300**.<br>**NOTA**<br>Si ha habilitado sesiones adhesivas y el servidor backend no responde dentro de la duración del tiempo de espera de respuesta, el balanceador de carga devuelve 504 Gateway Timeout a los clientes. | 60 |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy**.
   a. Se recomienda seleccionar un grupo de servidores backend existente.
   b. También puede hacer clic en **Create new** para crear un grupo de servidores backend y configurar los parámetros como se describe en **Tabla 2-17**.

**Tabla 2-17** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend debe ser TCP. | Create new |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group |
| Backend Protocol | Especifica el protocolo que utilizarán los servidores backend para recibir solicitudes.<br>El protocolo de backend es HTTP por defecto y no se puede cambiar. | HTTP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo que utilizará el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones activas establecidas con cada servidor backend, a cada servidor se le asigna una ponderación basada en su capacidad de procesamiento. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada se utiliza para asignar el cliente a un servidor en particular. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend. Este parámetro es opcional si ha seleccionado **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**. | N/D |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas para oyentes HTTP y HTTPS.<br>● **Load balancer cookie**: El balanceador de carga genera una cookie después de recibir una solicitud del cliente. Todas las solicitudes posteriores con la misma cookie se enrutan al mismo servidor back-end. | Load balancer cookie |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Slow Start | Especifica si se habilitará el inicio lento, que está deshabilitado de forma predeterminada.<br>Después de habilitar el inicio lento, el balanceador de carga aumenta linealmente la proporción de solicitudes para enviar a los servidores backend en este modo. Cuando transcurre la duración de inicio lento, el balanceador de carga envía una parte completa de las solicitudes a los servidores backend y sale del modo de inicio lento.<br>Para obtener más información, véase **Inicio lento (balanceadores de carga dedicados)**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Slow Start Duration | Especifica la duración de inicio lento si **Slow Start** está habilitado.<br>La duración varía de **30** a **1200** en segundos, y el valor predeterminado es **30**. | 30 |
| Description | Proporciona información adicional sobre el grupo de servidores backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para ver los parámetros necesarios para configurar una comprobación de estado, consulte **Tabla 2-18**.

**Tabla 2-18** Parámetros para configurar una comprobación de estado

| Parameter | Descripción | Example Value |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada, haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend.<br>Si el protocolo de backend es HTTP o HTTPS, el protocolo de comprobación de estado puede ser TCP, HTTP o HTTPS. | HTTP |

| Parameter | Descripción | Example Value |
| --- | --- | --- |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto oscila entre **1** y **65535**.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra inclinada (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras (/), puntos (.), signos de interrogación (?), signos numéricos (#), signos de porcentaje (%), ampersands (&) y conjuntos de caracteres extendidos _;~!.() *[]@ $^:',+ | /index.html |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |

| Parameter | Descripción | Example Value |
| --- | --- | --- |
| Timeout (s) | Specifies the maximum time required for waiting for a response from the health check, in seconds. The timeout duration ranges from **1** to **50**. | 3 |
| Maximum Retries | Specifies the maximum number of health check retries. The value ranges from **1** to **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

## Adición de un oyente de HTTP a un balanceador de carga compartido

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configure los parámetros basados en **Tabla 2-19**.

**Tabla 2-19** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Name | Especifica el nombre de oyente. | listener |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | HTTP |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Redirect | Especifica si se va a habilitar la redirección.<br>Redirige las solicitudes a un oyente de HTTPS cuando se usa HTTP como protocolo frontend. Si tiene oyentes HTTPS y HTTP, puede usar esta función para redirigir las solicitudes desde el oyente HTTP al oyente HTTPS para garantizar la seguridad.<br>Si crea una redirección para un oyente HTTP, el servidor backend devolverá HTTP 301 Move Permanently a los clientes. | N/A |
| Redirected To | Especifica el oyente de HTTPS al que se redirigen las solicitudes. | listener-9ecd (HTTPS/443) |
| **Configuración avanzada** | | |
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | Whitelist |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup-b2 |
| Idle Timeout | Especifica el período de tiempo que una conexión debe mantenerse activa, en segundos. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud.<br>La duración del tiempo de espera en reposo varía de **0** a **4000**. | 60 |
| Request Timeout | Especifica el período de tiempo (en segundos) después del cual el balanceador de carga cierra la conexión si el balanceador de carga no recibe una solicitud del cliente.<br>La duración del tiempo de espera de la solicitud varía de **1** a **300**. | 60 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Response Timeout | Un balanceador de carga envía una solicitud a un servidor backend. Si el servidor backend no responde dentro del período de tiempo de espera, el balanceador de carga envía la solicitud a otro servidor backend. Si el servidor backend no responde durante el reintento, el balanceador de carga devuelve el código de error HTTP 504 al cliente.<br>La duración del tiempo de espera de la solicitud varía de **1** a **300**.<br>**NOTA**<br>Si ha habilitado sesiones adhesivas y el servidor backend no responde dentro de la duración del tiempo de espera de respuesta, el balanceador de carga devuelve 504 Gateway Timeout a los clientes. | 60 |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy**. Tabla 2-20 describe los parámetros para configurar un grupo de servidores backend.

**Tabla 2-20** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend debe ser TCP. | **Create new** |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group |
| Backend Protocol | Especifica el protocolo que utilizarán los servidores backend para recibir solicitudes.<br>El protocolo de backend es HTTP por defecto y no se puede cambiar. | HTTP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo que utilizará el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones activas establecidas con cada servidor backend, a cada servidor se le asigna una ponderación basada en su capacidad de procesamiento. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada se utiliza para asignar el cliente a un servidor en particular. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend.<br>**NOTA**<br>Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** para **Load Balancing Algorithm**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas para oyentes HTTP y HTTPS.<br>● **Load balancer cookie**: El balanceador de carga genera una cookie después de recibir una solicitud del cliente. Todas las solicitudes posteriores con la misma cookie se enrutan al mismo servidor back-end.<br>● **Application cookie**: La aplicación desplegada en el servidor backend genera una cookie después de recibir la primera solicitud del cliente. Todas las solicitudes con la misma cookie generada por la aplicación backend se enrutan al mismo servidor backend. | Load balancer cookie |
| Cookie Name | Especifica el nombre de la cookie. Si selecciona **Application cookie**, introduzca un nombre de cookie. | cookieName-qsps |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Description | Proporciona información adicional sobre el grupo de servidores backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para ver los parámetros necesarios para configurar una comprobación de estado, consulte **Tabla 2-21**.

**Tabla 2-21** Parámetros para configurar una comprobación de estado

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada,<br>haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend. Hay dos opciones: TCP y HTTP. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra inclinada (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras diagonales (/), puntos (.), signos de interrogación (?), signos de porcentaje (%), ampersands (&) y guiones bajos (_). | /index.html |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Especifica el tiempo máximo necesario para esperar una respuesta de la comprobación de estado, en segundos. La duración del tiempo de espera varía de **1** a **50**. | 3 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Maximum Retries | Especifica el número máximo de reintentos de comprobación de estado. El valor oscila entre **1** y **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

# 2.6 Adición de un oyente de HTTPS

## Escenarios

Los oyentes de HTTPS son los más adecuados para aplicaciones que requieren una transmisión cifrada. Los balanceadores de carga descifran las solicitudes de HTTPS antes de enrutarlas a los servidores backend, que luego envían las solicitudes procesadas a los balanceadores de carga para la encriptación antes de que se envíen a los clientes.

Cuando agregue un oyente de HTTPS, asegúrese de que la subred del balanceador de carga tenga suficientes direcciones IP. Si las direcciones IP son insuficientes, agregue más subredes en la página de resumen del balanceador de carga. Después de seleccionar una subred, asegúrese de que las reglas de ACL no estén configuradas para esta subred. Si las reglas están configuradas, es posible que no se permitan los paquetes de las solicitudes.

## Restricciones

- Balanceadores de carga dedicados: Si el protocolo de oyente es HTTPS, el protocolo del grupo de servidores backend puede ser HTTP o HTTPS.
- Balanceadores de carga compartidos: Si el protocolo oyente es HTTPS, el protocolo del grupo de servidores backend es HTTP por defecto y no se puede cambiar.
- Si un balanceador de carga dedicado utiliza una especificación para el balanceo de carga de red (TCP/UDP), no puede crear un oyente de HTTPS.

## Adición de un oyente de HTTPS a un balanceador de carga dedicado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configure los parámetros basados en **Tabla 2-22**.

**Tabla 2-22** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Name | Especifica el nombre de oyente. | listener-pnqy |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | HTTPS |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |
| SSL Authentication | Especifica si desea que se autentifiquen los clientes y los servidores backend.<br>Hay dos opciones: **One-way authentication** y **Mutual authentication**.<br>● Si solo se requiere la autenticación del servidor, seleccione **One-way authentication**.<br>● Si desea que los clientes y el balanceador de carga se autentifiquen entre sí, seleccione **Mutual authentication**. Solo los clientes autenticados podrán acceder al balanceador de carga. | One-way authentication |
| Server Certificate | Especifica el certificado que utilizará el servidor backend para autenticar el cliente cuando se utilice HTTPS como protocolo frontend.<br>Tanto el certificado como la clave privada son necesarios.<br>Para obtener más información, véase **Adición de un certificado**. | N/A |
| CA Certificate | Especifica el certificado que utilizará el servidor backend para autenticar el cliente cuando **SSL Authentication** esté establecido en **Mutual authentication**.<br>Un certificado de CA es emitido por una entidad emisora de certificados (CA) y se utiliza para verificar el emisor del certificado. Si se requiere autenticación mutua HTTPS, las conexiones HTTPS solo se pueden establecer cuando el cliente proporciona un certificado emitido por un CA específico.<br>Para obtener más información, véase **Adición de un certificado**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Enable SNI | Especifica si se habilita el SNI cuando se utiliza HTTPS como protocolo frontend.<br>SNI es una extensión de TLS y se utiliza cuando un servidor utiliza varios nombres de dominio y certificados.<br>Esto permite al cliente enviar la información del nombre de dominio mientras envía una solicitud de protocolo de enlace SSL. Después de que el balanceador de carga recibe la solicitud, el balanceador de carga consulta el certificado correspondiente basado en el nombre de dominio y lo devuelve al cliente. Si no se encuentra ningún certificado, el balanceador de carga devolverá el certificado predeterminado. Para obtener más información, véase **Certificado de SNI (para oyentes de HTTPS)**. | N/A |
| SNI Certificate | Especifica el certificado asociado al nombre de dominio cuando el protocolo de interfaz es HTTPS y SNI está habilitado.<br>Seleccione un certificado existente o cree uno.<br>Para obtener más información, véase **Adición de un certificado**. | N/A |
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | Whitelist |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup-b2 |
| Transfer Client IP Address | Especifica si se deben transmitir las direcciones IP de los clientes a los servidores backend.<br>Esta función está habilitada para balanceadores de carga dedicados de forma predeterminada y no se puede deshabilitar. | Enabled |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Advanced Forwarding | Especifica si se debe habilitar la política de reenvío avanzado. Puede agregar políticas de reenvío avanzadas a oyentes HTTP o HTTPS para reenviar solicitudes a diferentes grupos de servidores backend según el método de solicitud HTTP, el encabezado HTTP, la cadena de consulta o el bloque CIDR, además de nombres de dominio y direcciones URL. | Enabled |
| **Configuración avanzada** | | |
| Security Policy | Especifica la política de seguridad que puede utilizar si selecciona HTTPS como protocolo frontend. Para obtener más información, consulte **Política de seguridad de TLS**. | TLS-1-0 |
| HTTP/2 | Especifica si desea utilizar HTTP/2 cuando seleccione **HTTPS** para **Frontend Protocol**. Para obtener más información, véase **HTTP/2**. | N/A |
| Transfer Load Balancer EIP | Especifica si se debe almacenar la EIP enlazada al balanceador de carga en el campo de encabezado X-Forwarded-ELB-IP y pasar este campo a los servidores backend. | N/A |
| Idle Timeout | Especifica el período de tiempo que una conexión debe mantenerse activa, en segundos. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud.<br>La duración del tiempo de espera en reposo varía de **0** a **4000**. | 60 |
| Request Timeout | Especifica el período de tiempo (en segundos) después del cual el balanceador de carga cierra la conexión si el balanceador de carga no recibe una solicitud del cliente.<br>La duración del tiempo de espera de la solicitud varía de **1** a **300**. | 60 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Response Timeout | Especifica el período de tiempo (en segundos) después del cual el balanceador de carga envía un error de 504 Gateway Timeout al cliente si el balanceador de carga no recibe respuesta del servidor backend después de enrutar una solicitud al servidor backend y no recibe respuesta tras intentar enrutar la misma solicitud a otros servidores backend.<br>La duración del tiempo de espera de la solicitud varía de **1** a **300**.<br>**NOTA**<br>Si ha habilitado sesiones adhesivas y el servidor backend no responde dentro de la duración del tiempo de espera de respuesta, el balanceador de carga devuelve 504 Gateway Timeout a los clientes. | 60 |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy**.
   a. Se recomienda seleccionar un grupo de servidores backend existente.
   b. También puede hacer clic en **Create new** para crear un grupo de servidores backend y configurar los parámetros como se describe en **Tabla 2-23**.

**Tabla 2-23** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend debe ser TCP. | Create new |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group-sq4v |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Protocol | Especifica el protocolo que utilizarán los servidores backend para recibir solicitudes.<br>El protocolo backend puede ser HTTP o HTTPS y cambiarse entre las dos opciones. | HTTP |
| Load Balancing Algorithm | Especifica el algoritmo que utilizará el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones activas establecidas con cada servidor backend, a cada servidor se le asigna una ponderación basada en su capacidad de procesamiento. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada se utiliza para asignar el cliente a un servidor en particular. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend.<br>Este parámetro es opcional si ha seleccionado **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Sticky Session Type | Especifica el tipo de sesiones adhesivas para oyentes HTTP y HTTPS.<br>● **Load balancer cookie**: El balanceador de carga genera una cookie después de recibir una solicitud del cliente. Todas las solicitudes posteriores con la misma cookie se enrutan al mismo servidor back-end. | Load balancer cookie |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Slow Start | Especifica si se habilitará el inicio lento, que está deshabilitado de forma predeterminada.<br>Después de habilitar el inicio lento, el balanceador de carga aumenta linealmente la proporción de solicitudes para enviar a los servidores backend en este modo. Cuando transcurre la duración de inicio lento, el balanceador de carga envía una parte completa de las solicitudes a los servidores backend y sale del modo de inicio lento.<br>Para obtener más información, véase **Inicio lento (balanceadores de carga dedicados)**. | N/A |
| Slow Start Duration | Especifica cuánto tiempo durará el inicio lento.<br>La duración varía de **30** a **1200** en segundos, y el valor predeterminado es **30**. | 30 |
| Description | Proporciona información adicional sobre el grupo de backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para obtener los parámetros necesarios a configurar una comprobación de estado, consulte **Tabla 2-24**.

**Tabla 2-24** Parámetros para configurar una comprobación de estado

| Parameter | Descripción | Example Value |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada, haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend.<br>Si el protocolo de backend es HTTP o HTTPS, el protocolo de comprobación de estado puede ser TCP, HTTP o HTTPS. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto oscila entre **1** y **65535**.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |

| Parameter | Descripción | Example Value |
| --- | --- | --- |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra inclinada (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras (/), puntos (.), signos de interrogación (?), signos numéricos (#), signos de porcentaje (%), ampersands (&) y conjuntos de caracteres extendidos _;~!.() *[]@ $^:',+ | /index.html |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Specifies the maximum time required for waiting for a response from the health check, in seconds. The timeout duration ranges from **1** to **50**. | 3 |
| Maximum Retries | Specifies the maximum number of health check retries. The value ranges from **1** to **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

## Adición de un oyente de HTTPS a un balanceador de carga compartido

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**. Configure los parámetros basados en **Tabla 2-25**.

**Tabla 2-25** Parámetros para configurar un oyente

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Name | Especifica el nombre de oyente. | listener-pnqy |
| Frontend Protocol | Especifica el protocolo que utilizará el balanceador de carga para recibir solicitudes de clientes. | HTTPS |
| Frontend Port | Especifica el puerto que utilizará el balanceador de carga para recibir solicitudes de clientes.<br>El número de puerto se encuentra dentro del rango de 1 a 65535. | 80 |
| SSL Authentication | Especifica si desea que se autentifiquen los clientes y los servidores backend.<br>Hay dos opciones: **One-way authentication** y **Mutual authentication**.<br>● Si solo se requiere la autenticación del servidor, seleccione **One-way authentication**.<br>● Si desea que los clientes y el balanceador de carga se autentifiquen entre sí, seleccione **Mutual authentication**. Solo los clientes autenticados podrán acceder al balanceador de carga. | One-way authentication |
| CA Certificate | Especifica el certificado que permite a los clientes y servidores backend autenticarse mutuamente.<br>Para obtener más información, véase **Adición de un certificado**. | N/A |
| Server Certificate | Especifica el certificado utilizado por el servidor para autenticar el cliente cuando se utiliza HTTPS como protocolo frontend.<br>Tanto el certificado como la clave privada son necesarios.<br>Para obtener más información, véase **Adición de un certificado**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Enable SNI | Especifica si se habilita el SNI cuando se utiliza HTTPS como protocolo frontend.<br>SNI es una extensión de TLS y se utiliza cuando un servidor utiliza varios nombres de dominio y certificados.<br>Esto permite al cliente enviar la información del nombre de dominio mientras envía una solicitud de protocolo de enlace SSL. Después de que el balanceador de carga recibe la solicitud, el balanceador de carga consulta el certificado correspondiente basado en el nombre de dominio y lo devuelve al cliente. Si no se encuentra ningún certificado, el balanceador de carga devolverá el certificado predeterminado. Para obtener más información, véase **Certificado de SNI (para oyentes de HTTPS)**. | N/A |
| SNI Certificate | Especifica el certificado asociado al nombre de dominio cuando el protocolo de interfaz es HTTPS y SNI está habilitado.<br>Seleccione un certificado existente o cree uno.<br>Para obtener más información, véase **Adición de un certificado**. | N/A |
| **Configuración avanzada** | | |
| Access Control | Especifica cómo se controla el acceso al oyente. Para obtener más información, véase **Control de acceso**. Las siguientes opciones están disponibles:<br>● **All IP addresses**<br>● **Blacklist**<br>● **Whitelist** | **Whitelist** |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Creación de un grupo de direcciones IP**. | ipGroup-b2 |
| HTTP/2 | Especifica si desea utilizar HTTP/2 cuando seleccione **HTTPS** para **Frontend Protocol**. Para obtener más información, véase **HTTP/2**. | N/A |
| Security Policy | Especifica la política de seguridad que puede utilizar si selecciona HTTPS como protocolo frontend. Hay cuatro opciones. Para obtener más información, consulte **Política de seguridad de TLS**. | TLS-1-2 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Idle Timeout | Especifica el período de tiempo que una conexión debe mantenerse activa, en segundos. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud.<br>La duración del tiempo de espera en reposo varía de **0** a **4000**. | 60 |
| Request Timeout | Especifica el período de tiempo (en segundos) después del cual el balanceador de carga cierra la conexión si el balanceador de carga no recibe una solicitud del cliente.<br>La duración del tiempo de espera de la solicitud varía de **1** a **300**. | 60 |
| Response Timeout | Especifica el período de tiempo (en segundos) después del cual el balanceador de carga envía un error de 504 Gateway Timeout al cliente si el balanceador de carga no recibe respuesta del servidor backend después de enrutar una solicitud al servidor backend y no recibe respuesta tras intentar enrutar la misma solicitud a otros servidores backend.<br>La duración del tiempo de espera de la solicitud varía de **1** a **300**.<br>**NOTA**<br>Si ha habilitado sesiones adhesivas y el servidor backend no responde dentro de la duración del tiempo de espera de respuesta, el balanceador de carga devuelve 504 Gateway Timeout a los clientes. | 60 |
| Description | Proporciona información complementaria sobre el oyente.<br>Puede introducir un máximo de 255 caracteres. | N/A |

6. Haga clic en **Next: Configure Request Routing Policy**. Tabla 2-26 describe los parámetros para configurar un grupo de servidores backend.

**Tabla 2-26** Parámetros para configurar un grupo de servidores backend

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Backend Server Group | Especifica un grupo de servidores con las mismas características para recibir solicitudes del balanceador de carga. Hay dos opciones disponibles:<br>● **Create new**<br>● **Use existing**<br>**NOTA**<br>Para asociar un grupo de servidor de backend existente, asegúrese de que no está en uso. Seleccione el grupo de servidor de backend con el protocolo correcto. Por ejemplo, si el protocolo frontend es TCP, el protocolo backend solo puede ser TCP. | **Create new** |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group-sq4v |
| Backend Protocol | Especifica el protocolo utilizado por los servidores backend para recibir solicitudes.<br>El protocolo de backend es HTTP por defecto y no se puede cambiar. | HTTP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo utilizado por el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: las solicitudes se enrutan a diferentes servidores en función de sus pesos, lo que indica el rendimiento del procesamiento del servidor. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones activas establecidas con cada servidor backend, a cada servidor se le asigna una ponderación basada en su capacidad de procesamiento. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada se utiliza para asignar el cliente a un servidor en particular. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>**NOTA**<br>● Elija un algoritmo adecuado basado en sus requisitos para una mejor distribución del tráfico.<br>● Para **Weighted round robin** o **Weighted least connections**, no se enviará ninguna solicitud a un servidor con una ponderación de 0. | Weighted round robin |
| Sticky Session | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend.<br>**NOTA**<br>Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** para **Load Balancing Algorithm**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas para oyentes HTTP y HTTPS.<br>● **Load balancer cookie**: El balanceador de carga genera una cookie después de recibir una solicitud del cliente. Todas las solicitudes posteriores con la misma cookie se enrutan al mismo servidor back-end.<br>● **Application cookie**: La aplicación desplegada en el servidor backend genera una cookie después de recibir la primera solicitud del cliente. Todas las solicitudes con la misma cookie generada por la aplicación backend se enrutan al mismo servidor backend. | Load balancer cookie |
| Cookie Name | Especifica el nombre de cookie. Si selecciona **Application cookie**, introduzca un nombre de cookie. | cookieName-qsps |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Solo puede habilitar las sesiones adhesivas si selecciona **Weighted round robin** para **Load Balancing Algorithm**.<br>● Duración de la adherencia en la capa 4: **1** a **60**<br>● Duración de la adherencia en la capa 7: **1** a **1440** | 20 |
| Description | Proporciona información adicional sobre el grupo de servidores backend.<br>Puede introducir un máximo de 255 caracteres. | N/A |

7. Haga clic en **Next: Add Backend Server**. Agregue servidores backend y configure la comprobación de estado para el grupo de servidores backend. Para obtener más información acerca de cómo agregar servidores de backend, consulte **Descripción general**. Para obtener los parámetros necesarios a configurar una comprobación de estado, consulte **Tabla 2-27**.

**Tabla 2-27** Parámetros para configurar una comprobación de estado

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada,<br>haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend. Hay dos opciones: TCP y HTTP. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra inclinada (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras diagonales (/), puntos (.), signos de interrogación (?), signos de porcentaje (%), ampersands (&) y guiones bajos (_). | /index.html |
| Interval (s) | Especifica el intervalo para enviar solicitudes de comprobación de estado, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Especifica el tiempo máximo necesario para esperar una respuesta de la comprobación de estado, en segundos. La duración del tiempo de espera varía de **1** a **50**. | 3 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Maximum Retries | Especifica el número máximo de reintentos de comprobación de estado. El valor oscila entre **1** y **10**. | 3 |

8. Haga clic en **Next: Confirm**.
9. Confirme la configuración y haga clic en **Submit**.

# 2.7 Adición de un oyente UDP (con un grupo de servidores Backend QUIC asociado)

## Escenarios

Si utiliza UDP como protocolo frontend, puede seleccionar QUIC como protocolo backend y seleccionar el ID de conexión para enrutar solicitudes con el mismo ID de conexión al mismo servidor backend. QUIC tiene las ventajas de baja latencia, alta confiabilidad y sin bloqueo de cabecera (bloqueo HOL), y es muy adecuado para Internet móvil. No es necesario establecer nuevas conexiones cuando se cambia entre una red Wi-Fi y una red de datos móviles.

NOTA

- Las versiones QUIC incluyen Q043, Q046 y Q050.
- Los oyentes UDP que usan QUIC como protocolo backend no admiten la fragmentación.

## Restricciones y limitaciones

- Solo los balanceadores de carga dedicados admiten el protocolo QUIC.
- Solo puede agregar UDP oyentes si desea usar QUIC como protocolo de backend.

## Adición de un oyente UDP con un grupo de servidores Backend QUIC asociado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.

   Seleccione **Network load balancing (TCP/UDP)** y seleccione una especificación para el balanceador de carga.
5. En **Listeners**, haga clic en **Add Listener**.
6. En el paso **Configure Listener**, establezca **Frontend Protocol** en **UDP** y configure otros parámetros según los requisitos del sitio y haga clic en **Next: Configure Request Routing Policy**.
7. En el paso **Configure Routing Policy**, establezca **Backend Protocol** en **QUIC** y configure otros parámetros según sea necesario.

8. Configure los parámetros y haga clic en **Submit.**

### Operaciones consecuentes

Después de agregar un oyente, asocia los servidores backend con el oyente realizando las operaciones de **Descripción general**.

## 2.8 Configuración de la protección de modificación para un oyente

### Escenario

Puede habilitar la protección de modificación para un oyente para evitar que se modifique o elimine.

### Restricciones

Si habilita la protección de modificación para un oyente, no podrá:

- Modificar la información básica y la política de reenvío del oyente.
- Cambiar el grupo de servidores backend predeterminado.
- Eliminar el oyente y su balanceador de carga.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de la ficha **Summary**, haga clic en **Configure** junto a **Modification Protection**.
7. En el cuadro de diálogo **Configure Modification Protection**, habilite **Modification Protection**.

NOTA

Desactive **Modification Protection** si desea modificar o eliminar un oyente.

## 2.9 Configuración de duraciones de tiempo de espera

### Escenarios

Puede configurar duraciones de tiempo de espera (tiempo de espera en reposo, tiempo de espera de solicitud y tiempo de espera de respuesta) para que sus oyentes satisfagan diversas

demandas. Por ejemplo, si el tamaño de una solicitud de un cliente HTTP o HTTPS es grande, puede aumentar la duración del tiempo de espera de la solicitud para asegurarse de que la solicitud se puede enrutar correctamente.

Para los balanceadores de carga compartidos, solo puede cambiar las duraciones de tiempo de espera de TCP, HTTP y HTTPS oyentes, pero no puede cambiar las duraciones de tiempo de espera de UDP oyentes.

Para balanceadores de carga dedicados, puede cambiar la duración del tiempo de espera de los oyentes de TCP, UDP, HTTP y HTTPS.

**Figura 2-1** Duración del tiempo de espera en la capa 7

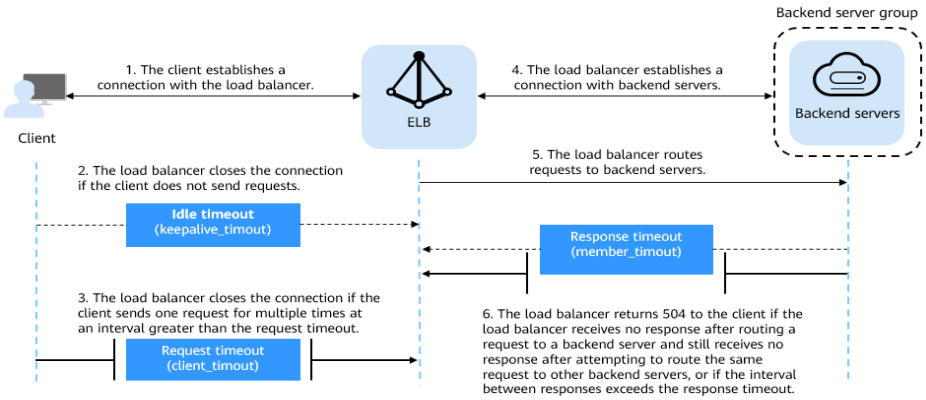



**Figura 2-2** Duración del tiempo de espera en la capa 4

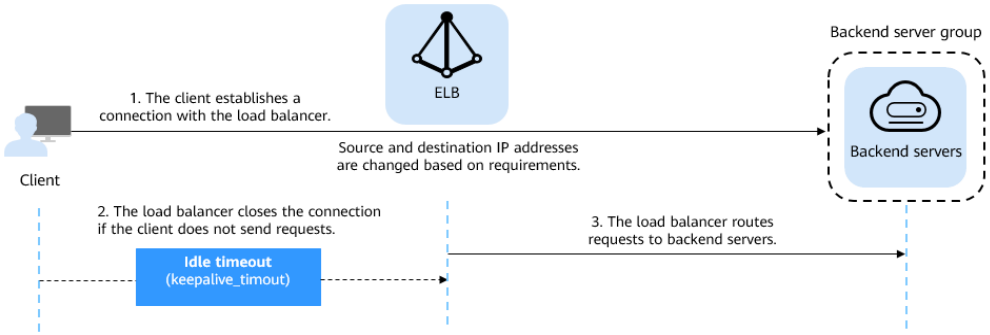


**Tabla 2-28** Duración del tiempo de espera

| Protocolo | Tipo | Descripción | Rango de valores | Duración de tiempo de espera por defecto |
|---|---|---|---|---|
| TCP | Período de expiración por inactividad | Duración para que una conexión se mantenga viva. Si no se recibe ninguna solicitud dentro de este período, el balanceador de carga cierra la conexión y establece una nueva con el cliente cuando llega la siguiente solicitud. | 10–4000s | 300s |
| UDP | Período de expiración por inactividad | | 10–4000s | Balanceadores de carga compartidos: 10s<br>Balanceadores de carga dedicados: 300s |
| HTTP/ HTTPS | Período de expiración por inactividad | | 10–4000s | 60s |
| | Tiempo de espera de solicitud | Duración después de la cual el balanceador de carga cierra la conexión con el cliente si el balanceador de carga no recibe una solicitud del cliente. | 10–300s | 60s |

| Protocolo | Tipo | Descripción | Rango de valores | Duración de tiempo de espera por defecto |
|---|---|---|---|---|
| | Tiempo de espera de la respuesta | Duración después de la cual el balanceador de carga envía un error 504 Gateway Timeout al cliente si el balanceador de carga no recibe respuesta después de encaminar una solicitud a un servidor backend y no recibe respuesta después de intentar encaminar la misma solicitud a otros servidores backend.<br>**NOTA**<br>Si las sesiones adhesivas están habilitadas y el servidor backend no responde dentro de la duración del tiempo de espera de respuesta, el balanceador de carga devuelve el código de error 504 sin intentar enrutar la misma solicitud a otros servidores backend. | 1–300s | 60s |

## Restricciones

Si la protección de modificación está habilitada para un oyente, sus duraciones de tiempo de espera no se pueden modificar.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en el nombre del oyente.
6. En la página de ficha **Summary**, haga clic en **Edit** en la parte superior derecha.
7. En el cuadro de diálogo **Edit**, expanda **Advanced Settings**.
8. Configure **Idle Timeout (s)**, **Request Timeout (s)** o **Response Timeout (s)** según lo necesite.

9. Haga clic en **OK**.

# 2.10 Modificación o eliminación de un oyente

## Escenarios

Puede modificar un oyente según sea necesario o eliminar un oyente si ya no lo necesita.

Los oyentes eliminados no se pueden recuperar.

NOTA

Frontend Protocol/Port y Backend Protocol no se pueden modificar después de que usted los ha configurado. Si desea modificar el protocolo o puerto del oyente, agregue otro oyente al balanceador de carga.

## Restricciones

Si la protección de modificación está habilitada para un oyente, el oyente no se puede eliminar o modificar.

## Modificación de un oyente

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Modifique el oyente de cualquiera de las siguientes maneras:
   - En la página **Listeners**, busque el oyente y haga clic en **Edit** en la columna **Operation**.
   - Haga clic en el nombre del oyente de destino. En la página de ficha **Summary**, haga clic en **Edit** en la esquina superior derecha.
6. En el cuadro de diálogo **Edit**, modifique los parámetros y haga clic en **OK**.

## Eliminación de un oyente

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.

NOTA

- Si el oyente tiene servidores backend asociados, desasocie los servidores backend antes de eliminar el oyente.
- Si las solicitudes HTTP se redirigen a un oyente de HTTPS, elimine la redirección antes de eliminar el oyente de HTTPS.
- Si el oyente tiene una política de reenvío, elimine la política de reenvío antes de eliminar el oyente.
- Después de eliminar un oyente, también se elimina el grupo de servidores backend asociado.

5. Haz clic en **Listeners**, localiza el oyente y haz clic en a la derecha de su nombre.
6. Haga clic en **Yes**.

# 2.11 Dirección IP del cliente de transferencia (balanceadores de carga dedicados)

## Transferir la dirección IP del cliente

Si habilita las **Transfer Client IP Address**, su balanceador de carga utilizará la dirección IP del cliente para acceder al servidor backend.

Tabla 2-29 muestra si puede habilitar o deshabilitar la función de dirección IP del cliente de transferencia.

**Tabla 2-29** Transferir la dirección IP del cliente

| Tipo de oyente | Habilitación de la dirección IP del cliente de transferencia | Desactivación de la dirección IP del cliente de transferencia |
|---|---|---|
| TCP y UDP | Habilitados por defecto | × |
| HTTP y HTTPS | Habilitados por defecto | × |

## Restricciones

- Si **Transfer Client IP Address** está habilitado, un servidor no puede servir como servidor backend y como cliente.

  Si el cliente y el servidor backend están usando el mismo servidor y la opción **Transfer Client IP Address** está activada, el servidor backend pensará que el paquete se envía por sí mismo, pero no desde el cliente y no devolverá un paquete de respuesta al balanceador de carga. Como resultado, el tráfico de retorno se interrumpirá.
- Después de activar esta función, la descarga unidireccional o el tráfico push pueden ser interrumpidos cuando se están migrando servidores backend. Después de migrar los servidores backend, retransmita los paquetes para restaurar el tráfico.
- Si agrega direcciones IP como servidores backend, las direcciones IP de origen de los clientes no se pueden pasar a estos servidores. Instale el **módulo TOA** para obtener direcciones IP de origen.

### Alternativas para obtener la dirección IP del cliente

Puede obtener la dirección IP de un cliente de una de las maneras indicadas en **Tabla 2-30**.

**Tabla 2-30** Alternativas

| Tipo de oyente | Alternativa |
| --- | --- |
| TCP y UDP | **Configuración del módulo TOA** |
| HTTP y HTTPS | **Equilibrio de carga de la capa 7** |

## 2.12 Transferir la dirección IP del cliente (balanceadores de carga compartidos)

### Escenario

Generalmente, los balanceadores de carga utilizan direcciones IP en 100.125.0.0/16 para comunicarse con servidores backend. Si desea que un balanceador de carga se comunique con los servidores backend utilizando direcciones IP reales de los clientes, puede habilitar **Transfer Client IP Address** para pasar las direcciones IP de los clientes a los servidores backend.

**Tabla 2-31** muestra si puede habilitar o deshabilitar la función de dirección IP del cliente de transferencia.

**Tabla 2-31** Transferir la dirección IP del cliente

| Tipo de oyente | Habilitación de la dirección IP del cliente de transferencia | Desactivación de la dirección IP del cliente de transferencia |
| --- | --- | --- |
| TCP y UDP | √ | √ |
| HTTP y HTTPS | Habilitados por defecto | × |

### Restricciones

- Al activar o desactivar la función, si el oyente tiene servidores backend asociados, el tráfico a este oyente se interrumpirá durante unos 10 segundos. La duración de la interrupción es el doble del intervalo de comprobación de estado configurado para el grupo de servidores backend.
- Si **Transfer Client IP Address** está habilitado, un servidor no puede servir como servidor backend y como cliente. Si el cliente y el servidor backend están usando el mismo servidor y la opción **Transfer Client IP Address** está activada, el servidor backend pensará que el paquete se envía por sí mismo, pero no desde el cliente y no devolverá un paquete de respuesta al balanceador de carga. Como resultado, el tráfico de retorno se interrumpirá.

- Si un servidor backend se ha asociado con el oyente y las comprobaciones de estado están habilitadas, al activar esta función se comprobará el estado del servidor backend, y el tráfico a este servidor se interrumpirá durante uno o dos intervalos de comprobación de estado.
- Después de activar esta función, la descarga unidireccional o el tráfico push pueden ser interrumpidos cuando se están migrando servidores backend. Después de migrar los servidores backend, retransmita los paquetes para restaurar el tráfico.

## Habilitación de la dirección IP del cliente de transferencia

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Puede utilizar cualquiera de los siguientes métodos para habilitar la función:
   - En la página **Listeners**, busque el oyente y haga clic en **Edit** en la columna **Operation**.
   - Haga clic en el nombre del oyente de destino. En la página de ficha **Summary**, haga clic en **Edit** en la esquina superior derecha.
6. En el cuadro de diálogo que se muestra, habilite **Transfer Client IP Address**.
7. Confirme las configuraciones y haga clic en **OK**.

NOTA

Después de habilitar **Transfer Client IP Address**, configure los grupos de seguridad, las ACL de red y las políticas de seguridad de SO y software para que las direcciones IP de los clientes puedan acceder a estos servidores backend.

## Desactivación de la dirección IP del cliente de transferencia

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Puede utilizar cualquiera de los siguientes métodos para deshabilitar la función:
   - En la página **Listeners**, busque el oyente y haga clic en **Edit** en la columna **Operation**.
   - Haga clic en el nombre del oyente de destino. En la página de ficha **Summary**, haga clic en **Edit** en la esquina superior derecha.
6. En el cuadro de diálogo que se muestra, deshabilite **Transfer Client IP Address**.
7. Confirme las configuraciones y haga clic en **OK**.

## Alternativas para obtener la dirección IP del cliente

Puede obtener la dirección IP de un cliente de una de las maneras indicadas en **Tabla 2-32**.

**Tabla 2-32** Alternativas

| Tipo de oyente | Alternativa |
| --- | --- |
| TCP y UDP | **Configuración del módulo TOA** |
| HTTP y HTTPS | **Equilibrio de carga de la capa 7** |

# 3 Características avanzadas de los oyentes de HTTP/HTTPS

## 3.1 Política de reenvío (balanceadores de carga compartidos)

### Escenarios

Puede agregar las políticas de reenvío a oyentes de HTTP o de HTTPS para reenviar solicitudes a diferentes grupos de servidores backend basados en nombres de dominio o URL.

Esto es adecuado para aplicaciones que se implementan en varios servidores backend y proporcionan múltiples tipos de servicios, como vídeos, imágenes, audios y textos.

Una política de reenvío consiste en una regla de reenvío y una acción.

- Hay dos tipos de reglas de reenvío: nombre de dominio y URL.
- Los oyentes de HTTP pueden reenviar solicitudes a un grupo de servidores backend y redirigir solicitudes a otro oyente.
- Los oyentes de HTTPS pueden reenviar solicitudes a un grupo de servidores backend.

### Cómo se combinan las solicitudes

- Después de agregar una política de reenvío, el balanceador de carga reenvía las solicitudes basadas en el nombre de dominio o URL especificado:
  - Si el nombre de dominio o la dirección URL de una solicitud coincide con el especificado en la política de reenvío, la solicitud se reenvía al grupo de servidores backend que seleccione o cree al agregar la política de reenvío.
  - Si el nombre de dominio o la URL de una solicitud no coinciden con lo especificado en la política de reenvío, la solicitud se reenvía al grupo de servidores backend predeterminado del oyente.
- Prioridad coincidente:
  - Las prioridades de las políticas de reenvío son independientes entre sí, independientemente de los nombres de dominio. Si una regla de reenvío utiliza

tanto nombres de dominio como los URL, las solicitudes se hacen coincidir en función de los nombres de dominio primero.

– Si la regla de reenvío es un URL, las prioridades siguen el orden de coincidencia exacta, coincidencia de prefijo y coincidencia de expresión regular. Si los tipos coincidentes son los mismos, cuanto mayor sea la longitud del URL, mayor será la prioridad.

**Tabla 3-1** Ejemplos de políticas de reenvío

| Solicitud | Política de reenvío | Regla de reenvío | Valor especificado |
|---|---|---|---|
| www.elb.com/test | 1 | URL | /test |
| | 2 | Nombre de dominio | www.elb.com |

NOTA

En este ejemplo, la solicitud **www.elb.com/test** coincide con las políticas de reenvío 1 y 2, pero se enruta según la política de reenvío 2.

## Restricciones y limitaciones

- Las políticas de reenvío solo se pueden agregar a los oyentes HTTP y HTTPS.
- Las políticas de reenvío deben ser únicas.
- Se puede configurar un máximo de 100 políticas de reenvío para un oyente. Si el número de políticas de reenvío excede la cuota, no se aplicarán las políticas de reenvío en exceso.
- Cuando agregue una política de reenvío, tenga en cuenta lo siguiente:
  – Cada ruta de URL debe existir en el servidor backend. Si la ruta no existe, el servidor backend devolverá 404 Not Found.
  – En la coincidencia de expresiones regulares, los caracteres se hacen coincidir secuencialmente y la coincidencia termina cuando cualquier regla se hace coincidir correctamente. Las reglas de coincidencia no pueden superponerse entre sí.
  – No se puede configurar una ruta de dirección URL para dos políticas de reenvío.
  – Un nombre de dominio no puede superar los 100 caracteres.

ATENCIÓN

Si agrega una política de reenvío que sea la misma que una existente invocando a las API, habrá un conflicto. Incluso si elimina la política de reenvío existente, la nueva política de reenvío sigue siendo defectuosa. Elimine la nueva política de reenvío agregada y agregue una diferente.

## Adición de una política de reenvío

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En la página de ficha **Listeners**, agregue una política de reenvío de cualquiera de las siguientes maneras:
   - En la página **Listeners**, busque el oyente y haga clic en **Add/Edit Forwarding Policy** en la columna **Forwarding Policies**.
   - Localice el oyente de destino, haga clic en su nombre y haga clic en **Forwarding Policies**.
6. Haga clic en **Add Forwarding Policy**. Configura los parámetros basados en **Tabla 3-2**.
7. Una vez completada la configuración, haga clic en **Save**.

**Tabla 3-2** Parámetros de política de reenvío

| Parámetro | | Descripción | Valor de ejemplo |
|---|---|---|---|
| Forwarding Rule | Domain name | Especifica el nombre de dominio utilizado para reenviar solicitudes. El nombre de dominio de la solicitud debe coincidir exactamente con el de la política de reenvío.<br>Debe especificar un nombre de dominio o un URL. | www.test.com |
| | URL | Especifica el URL utilizado para reenviar solicitudes. Hay tres reglas de coincidencia de URL:<br>● Coincidencia exacta<br>El URL de solicitud debe coincidir exactamente con la especificada en la política de reenvío.<br>● Coincidencia de prefijos<br>La URL solicitada comienza con la string URL especificada.<br>● Coincidencia de expresiones regulares<br>La URL solicitada coincide con la string de URL especificada basada en la expresión regular. | /login.php |

| Parámetro | | Descripción | Valor de ejemplo |
| --- | --- | --- | --- |
| Action | Forward to a backend server group | Si la solicitud coincide con la regla de reenvío configurada, la solicitud se reenvía al grupo de servidores backend especificado. | Reenvío a un grupo de servidores backend |
| | Redirect to another listener | Si la solicitud coincide con la regla de reenvío configurada, la solicitud se redirige al oyente especificado de HTTPS.<br>Esta acción solo se puede configurar para oyentes de HTTP.<br>**NOTA**<br>Si selecciona **Redirect to another oyente** y crea una redirección para el oyente actual, este oyente redirigirá las solicitudes al oyente de HTTPS especificado, pero el control de acceso configurado para el oyente seguirá teniendo efecto.<br>Por ejemplo, si configura una redirección para un oyente de HTTP, las solicitudes de HTTP para acceder a una página web serán redirigidas al oyente de HTTPS que seleccione y manejadas por los servidores backend asociados con el oyente de HTTPS. Como resultado, los clientes acceden a la página web con HTTPS. La configuración del oyente de HTTP no será válida. | N/A |
| Backend Server Group | | Seleccione un grupo de servidores backend que recibirá solicitudes del balanceador de carga.<br>Este parámetro es obligatorio cuando se establece **Action** en **Forward to a backend server group**. | N/A |
| Listener | | Seleccione un oyente de HTTPS que recibirá solicitudes redirigidas desde el oyente de HTTP actual.<br>Este parámetro es obligatorio cuando **Action** se establece en **Redirect to another listener**. | N/A |

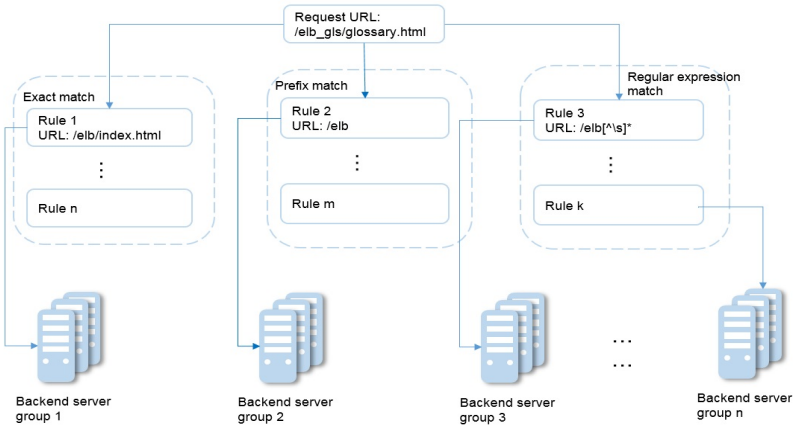
## Ejemplo de coincidencia de URL

En la siguiente tabla se muestra cómo se compara una dirección URL y **Figura 3-1** muestra cómo se reenvía una solicitud a un grupo de servidores backend.

**Tabla 3-3** Dirección URL coincidente

| Regla de coincidencia de URL | URL | URL en la política de reenvío | | | |
|---|---|---|---|---|---|
| N/A | N/A | /elb/index.html | /elb | /elb[^\s]* | /index.html |
| Coincidencia exacta | /elb/index.html | √ | N/A | N/A | N/A |
| Coincidencia de prefijos | | √ | √ | N/A | N/A |
| Coincidencia de expresiones regulares | | √ | N/A | √ | N/A |

**Figura 3-1** Solicitud de reenvío




En esta figura, el sistema primero busca una coincidencia exacta del URL solicitado (/elb_gls/glossary.html). Si no hay coincidencia exacta, el sistema busca una coincidencia de prefijo. Si se encuentra una coincidencia, la solicitud se reenvía al grupo 2 de servidores de backend incluso si también se encuentra una coincidencia de expresión regular, porque la coincidencia de prefijo tiene una prioridad más alta.

## Modificación de una política de reenvío

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Forwarding Policies**, seleccione la política de reenvío y haga clic en **Edit**.
7. Modifique los parámetros y haga clic en **Save**.

### Eliminación de una política de reenvío

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Forwarding Policies**, seleccione la política de reenvío y haga clic en **Delete** en la parte superior derecha.
7. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

## 3.2 Política de reenvío (balanceadores de carga dedicados)

### Descripción general

Puede agregar las políticas de reenvío a oyentes de HTTP o de HTTPS para reenviar solicitudes a diferentes grupos de servidores backend basados en nombres de dominio o URL.

Una política de reenvío consta de una o más reglas de reenvío y una acción. Para obtener más información, véase **Tabla 3-4**.

**Tabla 3-4** Reglas y acciones admitidas por una política de reenvío

| Tipo de política | Reglas de reenvío | Acciones |
|---|---|---|
| Política de reenvío | Nombre de dominio y URL | **Forward to another backend server group** y **Redirect to another oyente** (solo para oyentes de HTTP) |
| Política de reenvío avanzada | Nombre de dominio, URL, método de solicitud HTTP, encabezado de HTTP, cadena de consulta y bloque CIDR | **Forward to a backend server group**, **Redirect to another oyente**, **Redirect to another URL**, y **Return a specific response body** |

NOTA

Puede configurar una política de reenvío avanzada haciendo referencia a **Gestión de una política de reenvío avanzado**.

## Cómo se comparan las solicitudes

- Después de agregar una política de reenvío, el balanceador de carga reenvía las solicitudes basadas en el nombre de dominio o URL especificado:
  - Si el nombre de dominio o el URL de una solicitud coincide con el especificado en la política de reenvío, la solicitud se reenvía al grupo de servidores backend que cree o seleccione al agregar la política de reenvío.
  - Si el nombre de dominio o el URL de una solicitud no coinciden con lo especificado en la política de reenvío, la solicitud se reenvía al grupo de servidores backend predeterminado del oyente.
- Prioridad coincidente:
  - Las prioridades de las políticas de reenvío son independientes entre sí, independientemente de los nombres de dominio. Si una regla de reenvío utiliza tanto nombres de dominio como direcciones URL, las solicitudes se hacen coincidir en función de los nombres de dominio primero.
  - Si la regla de reenvío es un URL, las prioridades siguen el orden de coincidencia exacta, coincidencia de prefijo y coincidencia de expresión regular. Si los tipos coincidentes son los mismos, cuanto mayor sea la longitud del URL, mayor será la prioridad.

**Tabla 3-5** Ejemplos de políticas de reenvío

| Solicitud | Política de reenvío | Regla de reenvío | Valor especificado |
|---|---|---|---|
| www.elb.com/test | 1 | URL | /test |
| | 2 | Nombre de dominio | www.elb.com |

NOTA

En este ejemplo, la solicitud **www.elb.com/test** coincide con las políticas de reenvío 1 y 2, pero se enruta según la política de reenvío 2.

## Notas y restricciones

- Puede agregar políticas de reenvío a los oyentes HTTP y HTTPS.
- Las políticas de reenvío deben ser únicas.
- Se puede configurar un máximo de 100 políticas de reenvío para un oyente. Si el número de políticas de reenvío excede la cuota, no se aplicarán las políticas de reenvío en exceso.
- Cuando agregue una política de reenvío, tenga en cuenta lo siguiente:
  - Cada ruta de URL debe existir en el servidor backend. De lo contrario, el servidor backend devuelve 404 cuando se accede al servidor backend.

- En la coincidencia de expresiones regulares, las reglas se hacen coincidir secuencialmente y la coincidencia termina cuando cualquier regla se hace coincidir correctamente. Las reglas de coincidencia no pueden superponerse entre sí.
- No se puede configurar una ruta del URL para dos políticas de reenvío.
- Un nombre de dominio no puede superar los 100 caracteres.

## Adición de una política de reenvío

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en su nombre.
5. En la página de ficha **Listeners**, agregue una política de reenvío de cualquiera de las siguientes maneras:
   - Haga clic en **Add/Edit Forwarding Policy** en la columna **Forwarding Policies**.
   - Localice el oyente de destino, haga clic en su nombre y haga clic en **Forwarding Policies**.
6. Haga clic en **Add Forwarding Policy**. Configure los parámetros basados en **Tabla 3-6**.

**Tabla 3-6** Parámetros de política de reenvío

| Parámetro | Tipo | Descripción | Valor de ejemplo |
|---|---|---|---|
| Forwarding Rule | Nombre de dominio | Especifica el nombre de dominio utilizado para reenviar solicitudes. El nombre de dominio de la solicitud debe coincidir exactamente con el de la política de reenvío.<br>Debe especificar un nombre de dominio o un URL. | www.test.com |

| Parámetro | Tipo | Descripción | Valor de ejemplo |
|---|---|---|---|
| | URL | Especifica la dirección URL utilizada para reenviar solicitudes. Hay tres reglas de coincidencia de URL:<br>● Coincidencia exacta: el URL de solicitud debe coincidir exactamente con la especificada en la política de reenvío.<br>● Coincidencia de prefijo: El URL solicitado comienza con la cadena de URL especificada.<br>● Coincidencia de expresión regular: Los URL se hacen coincidir mediante una expresión regular. | /login.php |
| Action | Reenvío a un grupo de servidores backend | Si la solicitud coincide con la regla de reenvío configurada, la solicitud se reenvía al grupo de servidores backend especificado. | - |
| | Redirigir a otro oyente | Si la solicitud coincide con la regla de reenvío configurada, la solicitud se redirige al HTTPS oyente especificado.<br>Esta acción solo se puede configurar para oyentes HTTP.<br>**NOTA**<br>Si selecciona **Redirect to another oyente**, el oyente HTTP redirigirá las solicitudes al oyente HTTPS especificado, pero el control de acceso configurado para el oyente HTTP todavía tiene efecto. | - |

7. Haga clic en **Save**.

# 3.3 Reenvío avanzado (balanceadores de carga dedicados)

## 3.3.1 Reenvío avanzado

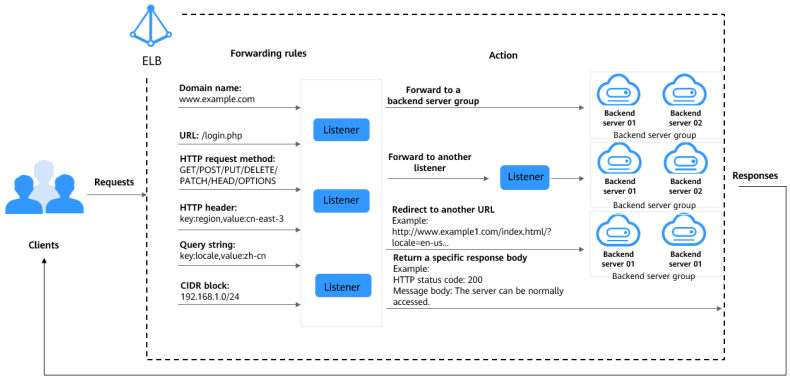
### Descripción general

Las políticas de reenvío avanzadas solo están disponibles para balanceadores de carga dedicados. Si ha habilitado **Advanced Forwarding**, puede agregar políticas de reenvío avanzadas a los oyentes HTTP y HTTPS de balanceadores de carga dedicados.

Puede agregar políticas de reenvío avanzadas a oyentes HTTP o HTTPS para reenviar solicitudes a diferentes grupos de servidores backend según el método de solicitud HTTP, el encabezado HTTP, la cadena de consulta o el bloque CIDR, además de nombres de dominio y direcciones URL. **Tabla 3-7** describe las reglas y acciones que puede configurar para el reenvío de solicitudes.

**Figura 3-2** Cómo funciona el reenvío avanzado




A continuación se describe cómo funciona una política de reenvío avanzada:

**Paso 1** El cliente envía una solicitud al balanceador de carga.

**Paso 2** El balanceador de carga coincide con la solicitud según la regla de reenvío que configure.

**Paso 3** El balanceador de carga reenvía la solicitud al servidor backend correspondiente o devuelve una respuesta fija al cliente basada en la acción que configure.

**Paso 4** El balanceador de carga envía una respuesta al cliente.

**----Fin**

**Tabla 3-7** Reglas y acciones apoyadas por una política de reenvío avanzado

| Política de reenvío | Descripción |
| --- | --- |
| Regla de reenvío | Hay seis tipos de reglas de reenvío: nombre de dominio, URL, método de solicitud HTTP, encabezado HTTP, cadena de consulta y bloque CIDR<br>Para obtener más información, véase **Regla de reenvío**. |
| Acción | Se admiten las siguientes acciones: reenviar a un grupo de servidores backend, redirigir a otro oyente, redirigir a otro URL y devolver un cuerpo de respuesta específico.<br>Para obtener más información, véase **Tipos de acción**. |

## Cómo se comparan las solicitudes

Después de agregar un oyente HTTP o HTTPS a un balanceador de carga, se genera una política de reenvío predeterminada. Esta política utiliza el protocolo y el puerto especificados

para que el oyente coincida con las solicitudes y reenvíe las solicitudes al grupo de servidores de backend que especificó al agregar el oyente.

La política de reenvío predeterminada tiene la prioridad más baja y no se incluye al ordenar las políticas de reenvío. Se puede editar pero no se puede eliminar.

Cada solicitud se hace coincidir basándose en la prioridad de la política de reenvío (un valor más pequeño indica una prioridad más alta). Una vez coincidente una política de reenvío, la solicitud se reenvía según esta política de reenvío.

- Si la solicitud coincide con cualquier política de reenvío del oyente, se reenvía según esta política de reenvío.
- Si la solicitud no coincide con ninguna política de reenvío, se reenvía según la política de reenvío predeterminada.

## Regla de reenvío

Las políticas de reenvío avanzadas admiten los siguientes tipos de reglas de reenvío: nombre de dominio, URL, método de solicitud HTTP, encabezado HTTP, consulta de string y bloque CIDR (direcciones IP de origen).

**Tabla 3-8** Reglas de reenvío

| Regla de reenvío | Descripción |
| --- | --- |
| Nombre de dominio | ● Descripción<br>Solicitudes de ruta basadas en el nombre de dominio.<br>– Puede configurar varios nombres de dominio en una política de reenvío. Cada nombre de dominio contiene al menos dos etiquetas separadas por puntos (.). Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres.<br>– Cada etiqueta puede contener letras, dígitos, guiones (-), puntos (.), y asteriscos (*). Una etiqueta debe comenzar con una letra, un dígito o un asterisco (*) y no puede terminar con un guion (-). Se debe usar un asterisco (*) como etiqueta situada más a la izquierda si desea configurar un nombre de dominio comodín.<br>● Reglas de coincidencia<br>Se admiten dominios de coincidencia exacta y dominios comodín.<br>`Example`<br>`Request URL: https://www.example.com/login.php?locale=en-us=#videos`<br>`Domain name in the forwarding rule: www.example.com` |

| Regla de reenvío | Descripción |
| --- | --- |
| URL | ● Descripción<br>Solicitudes de ruta basadas en URLs. Puede configurar varias direcciones URL en una política de reenvío. Una dirección URL puede contener letras, dígitos y caracteres especiales _~';@^-%# $.*+?,=!:\|\/()[]{}.<br>Si la dirección URL contiene caracteres especiales como signos de interrogación (?) o teclas de almohadilla (#), escape los caracteres especiales antes de configurar la regla de reenvío.<br>● Reglas de coincidencia<br>– Coincidencia exacta: el URL de solicitud debe coincidir exactamente con la especificada en la política de reenvío. El URL debe comenzar con una barra (/) y puede usar asteriscos (*) y signos de interrogación (?) como comodines.<br>– Coincidencia de prefijo: El URL solicitado comienza con la cadena de URL especificada. El URL debe comenzar con una barra (/) y puede usar asteriscos (*) y signos de interrogación (?) como caracteres comodín.<br>– Coincidencia de expresión regular: Los URL se hacen coincidir mediante una expresión regular.<br>Para obtener más información acerca de las reglas de coincidencia de direcciones URL, consulte **URL coincidente**.<br>`Example`<br>`Request URL: https://www.example.com/login.php?locale=en-us#videos`<br>`URL in the forwarding rule: /login.php` |
| Cadena de consulta | Solicitudes de ruta basadas en la consulta de string.<br>Una consulta de string consta de una clave y uno o más valores. Es necesario establecer la clave y los valores por separado.<br>● La clave solo puede contener letras, dígitos y characters especiales !$'()*+,./:;=?@^-_'<br>● Una clave puede tener uno o más valores. El valor puede contener letras, dígitos y characters especiales !$'()*+,./:;=?@^-_'<br>Asteriscos (*) y signos de interrogación (?) se pueden utilizar como caracteres comodín.<br>`Example`<br>`Request URL: https://www.example.com/login.php?locale=en-us#videos`<br>`A query string needs to be configured for the forwarding rule:`<br>`Key: locale`<br>`Value: en-us` |
| Método de solicitud de HTTP | Enrutar solicitudes basadas en el método de HTTP.<br>● Puede configurar varios métodos de solicitud en una política de reenvío.<br>● Los siguientes métodos están disponibles: GET, POST, PUT, DELETE, PATCH, HEAD y OPTIONS.<br>`Example`<br>`GET` |

| Regla de reenvío | Descripción |
| --- | --- |
| Encabezado HTTP | Solicitudes de ruta basadas en el encabezado HTTP.<br>Un encabezado HTTP consta de una clave y uno o más valores. Es necesario configurar la clave y los valores por separado.<br>● La clave puede contener solo letras, dígitos, guiones bajos (_), y guiones (-).<br>● Una clave puede tener uno o más valores. El valor puede contener letras, dígitos y characters especiales !#$%&'()*+,./:;<=>?@[]^-_'{\|}~ Asteriscos (*) y signos de interrogación (?) se pueden utilizar como caracteres comodín.<br>`Example`<br>`Key: Accept-Language`<br>`Value: en-us` |
| Bloque CIDR | Enrute las solicitudes basadas en las direcciones IP de origen desde donde se originan las solicitudes.<br>`Example`<br>`192.168.1.0/24 or 2020:50::44/127` |

## Tipos de acción

Las políticas de reenvío avanzadas admiten las siguientes acciones: reenviar a un grupo de servidores backend, redirigir a otro oyente, redirigir a otro URL y devolver un cuerpo de respuesta específico.

**Tabla 3-9** Acciones de una política de reenvío avanzado

| Acción | Descripción |
| --- | --- |
| Reenvío a un grupo de servidores backend | Las solicitudes se reenvían al grupo de servidores backend especificado. |
| Redirigir a otro oyente | Las solicitudes son redirigidas a otro oyente, que luego enruta las solicitudes a su grupo de servidores backend asociado.<br>**NOTA**<br>Si selecciona **Redirect to another oyente** y crea una redirección para el oyente, redirigirá las solicitudes al oyente de HTTPS especificado, pero el control de acceso configurado para el oyente seguirá teniendo efecto.<br>Por ejemplo, si configura una redirección para un oyente de HTTP, las solicitudes de HTTP para acceder a una página web serán redirigidas al oyente HTTPS que seleccione y manejadas por los servidores backend asociados con el oyente HTTPS. Como resultado, los clientes acceden a la página web a través de HTTPS. La configuración del HTTP oyente no será válida. |

| Acción | Descripción |
| --- | --- |
| Redirigir a otro URL | Las solicitudes se redirigen al URL configurado.<br>Cuando los clientes acceden al sitio web A, el balanceador de carga devuelve 302 o cualquier otro código de estado 3xx y redirige automáticamente a los clientes al sitio web B. Puede personalizar el URL de redirección que se devolverá a los clientes.<br>Configure al menos uno de los siguientes componentes:<br>● **Protocol**: ${protocol}, HTTP o HTTPS **${protocol}**: conserva el protocolo de la solicitud.<br>● **Domain name**: Un nombre de dominio consta de al menos dos etiquetas separadas por puntos (.). Cada etiqueta puede contener solo letras, dígitos, guiones (-) y puntos (.), debe comenzar con una letra, dígito o asterisco (*), y no puede terminar con un guion (-). **${host}**: conserva el nombre de dominio de la solicitud.<br>● **Port**: oscila entre 1 y 65535. **${port}**: conserva el número de puerto de la solicitud.<br>● **Path**: Una ruta puede contener letras, dígitos y caracteres especiales _~';@^-%#&$.*+?,=!:\|\/()[]{} y debe comenzar con una barra diagonal (/). **${path}**: conserva la ruta de la solicitud.<br>**NOTA**<br>Si selecciona la coincidencia de expresiones regulares, la ruta de la solicitud se sobrescribirá con las variables que coincidan con las expresiones regulares.<br>● **Query String**: Una cadena de consulta puede contener solo letras, dígitos y characters !$'()*+,./:;=?@&^-_'. Ampersand (&) solo se puede utilizar como separadores.<br>● **HTTP status code**: 301, 302, 303, 307 o 308<br>`Example`<br>`URL for redirection: http://www.example1.com/index.html?locale=en-us#videos`<br>`Protocol: HTTP`<br>`Domain name: www.example1.com`<br>`Port: 8081`<br>`Path: /index.html`<br>`Query String: locale=en-us`<br>`HTTP Status Code: 301` |

| Acción | Descripción |
| --- | --- |
| Devolver un cuerpo de respuesta específico | Los balanceadores de carga devuelven una respuesta fija a los clientes.<br>Puede personalizar el código de estado y el cuerpo de respuesta que los balanceadores de carga devuelven directamente a los clientes sin necesidad de enrutar las solicitudes a los servidores backend.<br>Configure los siguientes componentes:<br>● **HTTP Status Code**: De forma predeterminada, se admiten códigos de estado 2xx, 4xx y 5xx.<br>● **Content-Type**: text/plain, text/css, text/html, application/javascript o application/json<br>● **Message body**: Este parámetro es opcional.<br>Ejemplo<br>text/plain<br>`Sorry, the language is not supported.`<br>text/css<br>`<head><style type="text/css">div {background-color:red}#div {font-size:15px;color:red}</style></head>`<br>text/html<br>`<form action="/" method="post" enctype="multipart/form-data"><input type="text" name="description" value="some text"><input type="file" name="myFile"><button type="submit">Submit</button></form>`<br>application/javascript<br>`String.prototype.trim = function() {var reExtraSpace = /^\s*(.*?)\s+$/;return this.replace(reExtraSpace, "$1")}`<br>application/json<br>`{ "publicip": { "type": "5_bgp","ip_version": 4},"bandwidth": {"name": "bandwidth123","size": 10,"share_type": "PER"}}`<br>**NOTA**<br>Asegúrese de que el cuerpo de la respuesta no contiene caracteres de retorno de carro. De lo contrario, no se puede guardar. |

## URL coincidente

**Tabla 3-10** muestra cómo los URL configurados en las políticas de reenvío coinciden con los URL de las solicitudes.

**Tabla 3-10** Ejemplos de coincidencia de URL

| URL de solicitud | Política de reenvío | URL en la política de reenvío | Modo de coincidencia | Prioridad de la política de reenvío | Grupo de servidores backend de destino |
|---|---|---|---|---|---|
| /elb/abc.html | Política de reenvío 01 | /elb/abc.html | Coincidencia de prefijos | 1 | Grupo de servidores backend 01 |
| | Política de reenvío 02 | /elb | Coincidencia de prefijos | 2 | Grupo de servidores backend 02 |
| /exa/index.html | Política de reenvío 03 | /exa[^\s]* | Coincidencia de expresiones regulares | 3 | Grupo de servidores backend 03 |
| | Política de reenvío 04 | /exa/index.html | Coincidencia de expresiones regulares | 4 | Grupo de servidores backend 04 |
| /mpl/index.html | Política de reenvío 05 | /mpl/index.html | Coincidencia exacta | 5 | Grupo de servidores backend 05 |

Los URL se coinciden de la siguiente manera:

- Cuando el URL de solicitud es /elb/abc.html, coincide con la política de reenvío 01 y la política de reenvío 02. Sin embargo, la prioridad de la política de reenvío 01 es mayor que la de la política de reenvío 02. Se utiliza la política de reenvío 01, y las solicitudes se reenvían al grupo de servidores backend 01.
- Cuando la URL de solicitud es /exa/index.html, coincide con la política de reenvío 03 y la política de reenvío 04. Sin embargo, la prioridad de la política de reenvío 03 es mayor que la de la política de reenvío 04. Se utiliza la política de reenvío 03, y las solicitudes se reenvían al grupo de servidores backend 03.
- Si la URL de solicitud es /mpl/index.html, coincide exactamente con la política de reenvío 05, y las solicitudes se reenvían al grupo de servidores backend 05.

## Coincidencia de URL basada en expresiones regulares

Una ruta puede contener letras, dígitos y caracteres especiales _~';@^-%#&$.*+?,=!:|\/()[]{} y debe comenzar con una barra diagonal (/). **${path}** conserva la ruta de la solicitud.

Si selecciona la coincidencia de expresiones regulares, la ruta de la solicitud se sobrescribirá con las variables que coincidan con las expresiones regulares.

**Cómo se sobrescriben las rutas solicitadas**

1. Coincidencia de URL: el cliente envía una solicitud, y la solicitud coincide con una expresión regular en la regla de reenvío. Puede especificar una o más expresiones regulares como condiciones de coincidencia y establecer varios grupos de captura representados por paréntesis **( )** para una expresión regular.
2. Extracción y sustitución: extrae el contenido de los grupos de captura.
3. Ruta de destino: los escribe a $1, $2, hasta $9 configurados para la ruta.

**Ejemplo**

Cuando un cliente solicita acceso a **/test/ELB/elb/index** que coincide con la expresión regular, **/test/(.*)/(.*)/index**, **$1** será reemplazada por **ELB** y **$2** por **elb** y luego la solicitud será redirigida a **/ELB/elb**.

**Tabla 3-11** Coincidencia de URL basada en expresiones regulares

| Paso de combinación | | Descripción |
|---|---|---|
| Regla de reenvío: URL | Coincidencia de expresiones regulares | ● Condición de combinación: /test/(.*)/(.*)/index<br>● URL de solicitud: /test/ELB/elb/index |
| Acción: Redireccionar a otro URL | Ruta | ● Ruta: /$1/$2<br>● Extracción de contenido<br>$1: ELB<br>$2: elb<br>● Ruta de destino: /ELB/elb |

# 3.3.2 Gestión de una política de reenvío avanzado

## Escenarios

Puede agregar políticas de reenvío avanzado a oyentes HTTP o HTTPS de balanceadores de carga dedicados para enrutar las solicitudes más específicamente.

Cada política de reenvío avanzado consta de una o más reglas de reenvío y una acción.

- Los balanceadores de carga dedicados admiten los siguientes tipos de reglas de reenvío: nombre de dominio, URL, método de solicitud HTTP, encabezado HTTP, string de consulta y bloque CIDR (direcciones IP de origen). Para obtener más información, véase **Regla de reenvío**.

- Hay cuatro tipos de acciones: reenviar a un grupo de servidores backend, redirigir a otro oyente, redirigir a otro URL y devolver un cuerpo de respuesta específico. Para obtener más información, véase **Tipos de acción**.
- Se pueden configurar varias reglas de reenvío en una sola política de reenvío.
- Las políticas de reenvío se pueden ordenar en función de sus prioridades.

## Restricciones

- El reenvío avanzado no se puede deshabilitar una vez habilitado.
- Un política de reenvío avanzado puede contener un máximo de 10 condiciones.

## Habilitación de reenvío avanzado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en la pestaña **Listeners** y haga clic en el oyente de destino.
6. En la página de la ficha **Summary**, haga clic en **Enable** junto a **Advanced Forwarding**.
7. Haga clic en **OK**.

## Adición de una política de reenvío avanzada

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en su nombre.
5. En la página de ficha **Listeners**, agregue una política de reenvío de cualquiera de las siguientes maneras:
   - Haga clic en **Add/Edit Forwarding Policy** en la columna **Forwarding Policies**.
   - Localice el oyente de destino, haga clic en su nombre y haga clic en **Forwarding Policies**.
6. Haga clic en **Add Forwarding Policy** y configure los parámetros basados en **Tabla 3-8** y **Tabla 3-9**.
7. Haga clic en **Save**.

## Ordenación de políticas de reenvío

Se pueden ordenar varias políticas de reenvío para establecer sus prioridades.

1. Inicie sesión en la consola de gestión.

2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de la ficha **Forwarding Policies**, haga clic en **Sort**.
7. Arrastre las políticas de reenvío para ajustar sus prioridades.
8. Haga clic en **Save**.

## Modificación de una política de reenvío

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Forwarding Policies**, seleccione la política de reenvío y haga clic en **Edit**.
7. Modifique los parámetros y haga clic en **Save**.

## Eliminación de una política de reenvío

Puede eliminar una política de reenvío si ya no la necesita.

No se pueden recuperar las políticas de enrutamiento eliminadas.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Forwarding Policies**, seleccione la política de reenvío y haga clic en **Delete** en la parte superior derecha.
7. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

# 3.4 Autenticación mutua

## Escenarios

En escenarios comunes de servicio HTTPS, solo se requiere el certificado de servidor para la autenticación. Para algunos servicios de misión crítica, como las transacciones financieras, debe desplegar tanto el certificado de servidor como el certificado de cliente para la autenticación mutua.

Los certificados autofirmados se utilizan como ejemplo para describir cómo configurar la autenticación mutua. Los certificados autofirmados no proporcionan todas las propiedades de seguridad proporcionadas por los certificados firmados por una CA. Se recomienda que compre certificados de **SSL Certificate Manager (SCM)** o CA.

## Creación de un certificado de CA mediante OpenSSL

1. Inicie sesión en un servidor Linux con OpenSSL instalado.
2. Cree el directorio **server** y cambie al directorio:

   **mkdir ca**

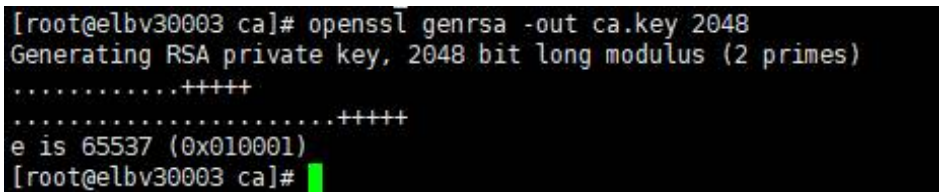
   **cd ca**
3. Cree el archivo de configuración del certificado **ca_cert.conf**. El contenido del archivo es el siguiente:

```
[ req ]
distinguished_name     = req_distinguished_name
prompt                 = no
[ req_distinguished_name ]
 O                      = ELB
```

4. Cree la clave privada del certificado de CA **ca.key**.

   **openssl genrsa -out ca.key 2048**

   **Figura 3-3** Clave privada del certificado de CA

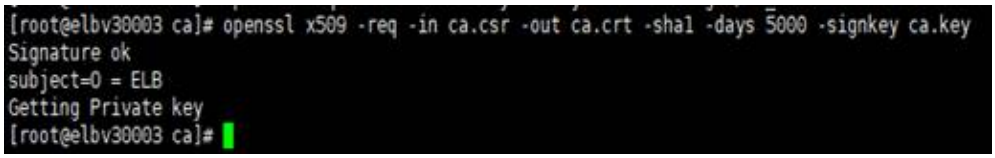



5. Cree el archivo de solicitud de firma de certificado (CSR) **ca.csr** para el certificado de CA.

   **openssl req -out ca.csr -key ca.key -new -config ./ca_cert.conf**
6. Cree el certificado CA autofirmado **ca.crt**.

   **openssl x509 -req -in ca.csr -out ca.crt -sha1 -days 5000 -signkey ca.key**

   **Figura 3-4** Creación de un certificado de CA autofirmado



## Emisión de un certificado de servidor mediante el certificado de CA

El certificado de servidor puede ser un certificado firmado por CA o uno autofirmado. En los pasos siguientes, se utiliza un certificado autofirmado como ejemplo para describir cómo crear un certificado de servidor.

1. Inicie sesión en el servidor donde se genera el certificado de CA.
2. Cree un directorio en el mismo nivel que el directorio del certificado de CA y cambie al directorio.

   **mkdir server**

   **cd server**
3. Cree el archivo de configuración de certificado **server_cert.conf**. El contenido del archivo es el siguiente:

```
[ req ]
distinguished_name     = req_distinguished_name
prompt                 = no
[ req_distinguished_name ]
 O                      = ELB
 CN                     = www.test.com
```

   NOTA

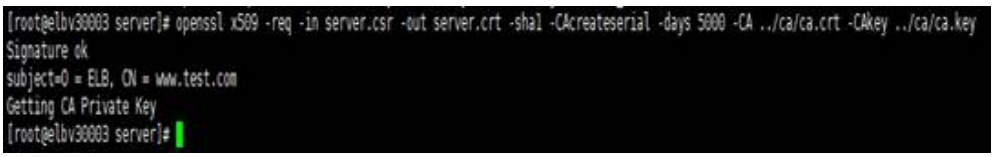
   Establezca el campo CN en el nombre de dominio o la dirección IP del servidor Linux.
4. Cree la clave privada de certificado de servidor server.key.

   **openssl genrsa -out server.key 2048**
5. Cree el archivo CSR **server.csr** para el certificado de servidor.

   **openssl req -out server.csr -key server.key -new -config ./server_cert.conf**
6. Utilice el certificado de CA para emitir el certificado de servidor **server.crt**.

   **openssl x509 -req -in server.csr -out server.crt -sha1 -CAcreateserial -days 5000 -CA ../ca/ca.crt -CAkey ../ca/ca.key**

**Figura 3-5** Emisión de un certificado de servidor




## Emisión de un certificado de cliente mediante el certificado de CA

1. Inicie sesión en el servidor donde se genera el certificado de CA.
2. Cree un directorio en el mismo nivel que el directorio del certificado de CA y cambie al directorio.

   **mkdir client**

   **cd client**
3. Cree el archivo de configuración de certificado **client_cert.conf**. El contenido del archivo es el siguiente:

```
[ req ]
distinguished_name     = req_distinguished_name
prompt                 = no
[ req_distinguished_name ]
 O                      = ELB
 CN                     = www.test.com
```

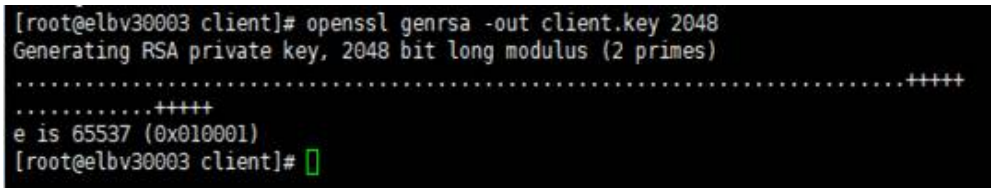
NOTA

Establezca el campo CN en el nombre de dominio o la dirección IP del servidor Linux.

4. Cree la clave privada del certificado de cliente **client.key**.

   **openssl genrsa -out client.key 2048**

   **Figura 3-6** Creación de una clave privada de certificado de cliente

5. Cree el archivo CSR **client.csr** para el certificado de cliente.

   **openssl req -out client.csr -key client.key -new -config ./client_cert.conf**

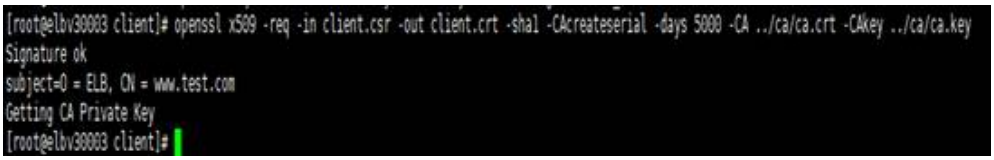
   **Figura 3-7** Creación de un archivo CSR de certificado de cliente

6. Utilice el certificado de CA para emitir el certificado de cliente **client.crt**.

   **openssl x509 -req -in client.csr -out client.crt -sha1 -CAcreateserial -days 5000 -CA ../ca/ca.crt -CAkey ../ca/ca.key**

   **Figura 3-8** Emisión de un certificado de cliente

7. Convierta el certificado de cliente en un archivo a .**p12** que pueda identificar el navegador.

   **openssl pkcs12 -export -clcerts -in client.crt -inkey client.key -out client.p12**

   NOTA

   Se requiere una contraseña durante la ejecución del comando. Guarde esta contraseña, que será necesaria cuando importe el certificado mediante el navegador.

## Configuración del certificado del servidor y la clave privada

1. Inicie sesión en la consola de gestión del balanceador de carga.
2. En el panel de navegación de la izquierda, elija **Certificates**.
3. En el panel de navegación de la izquierda, elija **Certificates**. En la página mostrada, haga clic en **Add Certificate**. En el cuadro de diálogo **Add Certificate**, seleccione **Server certificate** y copie el contenido del certificado de servidor **server.crt** en el área **Certificate Content** y el contenido del archivo de clave privada **server.key** en el área **Private Key** y haga clic en **OK**.

   NOTA

   Elimine el último carácter de nueva línea antes de copiar el contenido.

NOTA

El certificado y la clave privada deben estar codificados por PEM.

## Configuración del certificado de CA

**Paso 1** Inicie sesión en la consola de gestión del balanceador de carga.

**Paso 2** En el panel de navegación de la izquierda, elija **Certificates**.

**Paso 3** Haga clic en **Add Certificate**. En el cuadro de diálogo **Add Certificate**, seleccione **CA certificate**, copie el contenido del certificado de CA **ca.crt** creado en **Creación de un certificado de CA mediante OpenSSL** en el área **Certificate Content** y haga clic en **OK**.

NOTA

Elimine el último carácter de nueva línea antes de copiar el contenido.

NOTA

El certificado debe estar codificado por PEM.

**----Fin**

## Configuración de la Autenticación Mutua

1. Inicie sesión en la consola de gestión del balanceador de carga.
2. Busque el balanceador de carga y haga clic en su nombre. En **Listeners**, haga clic en **Add Listener**. Seleccione **HTTPS** para **Frontend Protocol** y **Mutual authentication** para **SSL Authentication** y seleccione un certificado de CA y un certificado de servidor.

**Agregar servidores de backend**.

Para obtener información detallada sobre las operaciones, consulte **Descripción general**.

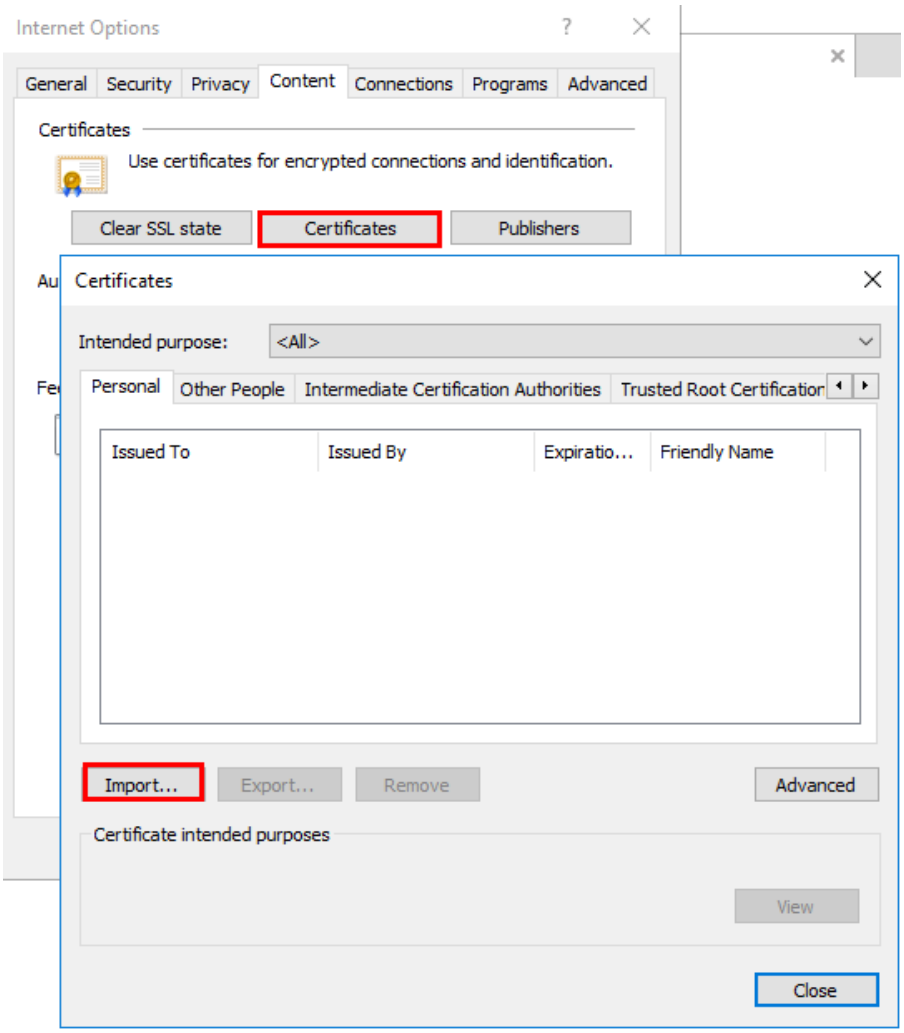
## Importación y prueba del certificado de cliente

Método 1: Uso de un navegador

1. Importe el certificado de cliente mediante un navegador (Internet Explorer 11 se utiliza como ejemplo).
   a. Exporte **client.p12** desde el servidor Linux.
   b. Abra el navegador, seleccione **Settings** > **Internet Options** y haga clic en **Content**.
   c. Haga clic en **Certificates** y, a continuación, **Import** para importar el certificado **client.p12**.

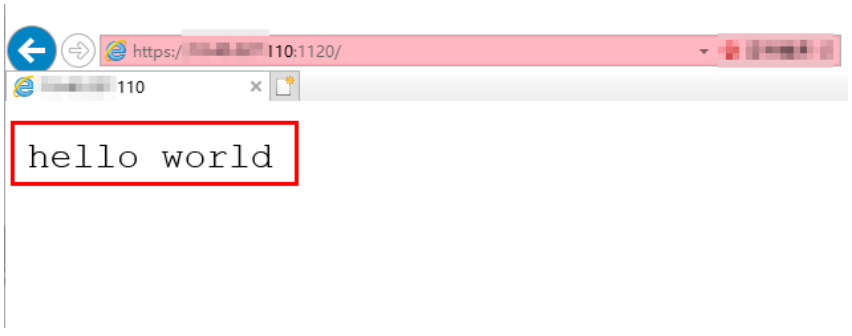
**Figura 3-9** Importación del certificado client.p12




2. Verifique la importación.

   Introduzca la dirección de acceso en el cuadro de dirección de su navegador. Aparece una ventana en la que se le pide que seleccione el certificado. Seleccione el certificado de cliente y haga clic en **OK**. Si se puede acceder al sitio web, el certificado se importa correctamente.

**Figura 3-10** Acceder al sitio web




Método 2: Usando cURL

1. Importe el certificado de cliente.

   Copie el certificado de cliente **client.crt** y la clave privada **client.key** en un nuevo directorio, por ejemplo, **/home/client_cert**.

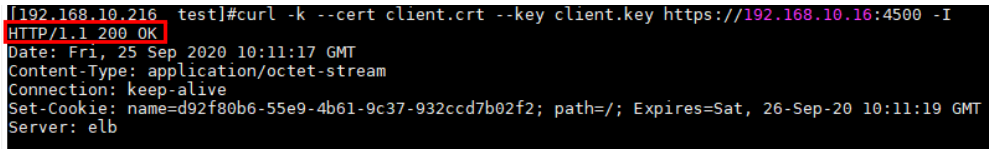
2. Verifique la importación.

   En la pantalla Shell, ejecute el siguiente comando:

   ```
   curl -k --cert /home/client_cert/client.crt --key /home/client_cert/
   client.key https://XXX.XXX.XXX.XXX:XXX/ -I
   ```

   Asegúrese de que la dirección del certificado, la dirección de clave privada, la dirección IP y el puerto de escucha del balanceador de carga sean correctos. Reemplace **https://XXX.XXX.XXX.XXX:XXX** con la dirección IP y el número de puerto reales. Si se devuelve el código de respuesta esperado, el certificado se importa correctamente.

   **Figura 3-11** Ejemplo de un código de respuesta correcto

# 3.5 HTTP/2

## Escenarios

Hypertext Transfer Protocol 2.0 (HTTP/2) es el protocolo HTTP de próxima generación. HTTP/2 se utiliza para proteger las conexiones entre el balanceador de carga y los clientes. Puede habilitar HTTP/2 cuando agrega oyentes de HTTPS. Si ya ha agregado un oyente HTTPS, también puede habilitar esta función.

## Restricciones

Puede habilitar HTTP/2 solo para oyentes de HTTPS.

## Habilitación de HTTP/2 al agregar un oyente

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**.
6. En el cuadro de diálogo **Add Listener**, establezca **Frontend Protocol** en **HTTPS**.
7. Expanda **Advanced Settings** y habilite HTTP/2.
8. Confirme las configuraciones y haga clic en **Submit**.

### Habilitar o deshabilitar HTTP/2 al modificar un oyente

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Summary**, haga clic en **Edit** en la parte superior derecha.
7. En el cuadro de diálogo **Edit**, expanda **Advanced Settings** y habilite o deshabilite HTTP/2.
8. Haga clic en **OK**.

## 3.6 Redirección de HTTP a HTTPS

### Escenarios

HTTPS es una extensión de HTTP. HTTPS cifra los datos entre un servidor web y un navegador.

Si habilita la redirección, todas las solicitudes HTTP a su sitio web se transmiten a través de conexiones HTTPS para mejorar la seguridad.

**ATENCIÓN**

- Si el protocolo oyente es HTTP, solo se puede usar el método GET o HEAD para la redirección. Si crea una redirección para un oyente HTTP, el navegador del cliente cambiará POST u otros métodos a GET. Si desea utilizar otros métodos en lugar de GET y HEAD, agregue un oyente de HTTPS.
- Las solicitudes HTTP se reenvían al oyente HTTPS como solicitudes HTTPS, que luego se enrutan a los servidores backend a través de HTTP.
- Si un oyente de HTTP es redirigido a un oyente de HTTPS, no se puede desplegar ningún certificado en los servidores backend asociados con el oyente de HTTPS. Si se implementan certificados, las solicitudes HTTPS no surtirán efecto.

### Requisitos previos

- Ha agregado un oyente HTTPS.
- Ha agregado un oyente HTTP.

### Creación de redirección a HTTPS

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

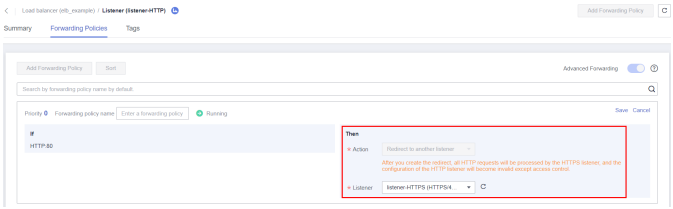
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente HTTP y haga clic en su nombre.
6. En la página de la ficha **Forwarding Policies**, haga clic en **Add Forwarding Policy**.

**Tabla 3-12** Configuración de parámetros para la redirección

| Parámetro | Configuración |
| --- | --- |
| Action | Seleccione **Redirect to another oyente**. |
| Listener | Seleccione el oyente de HTTPS al que se redirigen las solicitudes. |

7. Después de agregar la política de reenvío, haga clic en **Save**.

**Figura 3-12** Redirección a un oyente de HTTPS



NOTA

- Si las solicitudes a un oyente de HTTP son redirigidas, el oyente quedará inválido, pero el control de acceso al oyente todavía tendrá efecto.
- Si crea una redirección para un oyente HTTP, el servidor backend devolverá HTTP 301 Move Permanently a los clientes.

## Modificación de la redirección a HTTPS

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente HTTP y haga clic en su nombre.
6. En la página de ficha **Forwarding Policies**, busque la política de reenvío de destino y haga clic en **Edit**.
7. Puede cambiar el oyente de HTTPS al que se redirigen las solicitudes según sea necesario.

8. Haga clic en **Save**.

## Eliminación de redireccionamiento a HTTPS

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Forwarding Policies**, haga clic en **Delete** a la derecha de la política de reenvío de destino.
7. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

# 3.7 Transferencia del EIP del balanceador de carga a los servidores backend

## Escenarios

ELB permite que los EIP de los balanceadores de carga se pasen a los servidores backend. Puede habilitar la función cuando agrega HTTPS o HTTP oyentes.

Los EIP del balanceador de carga se colocan en el campo X-Forwarded-ELB-IP en el encabezado HTTPS o HTTP en el formato *XX.XXX.XX.XXX*, como se muestra a continuación:

```
X-Forwarded-ELB-IP: XX.XXX.XX.XXX
```

## Habilitación de la función

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**.
6. En el cuadro de diálogo **Add Listener**, expanda **Advanced Settings** y habilite la función.
7. Confirme las configuraciones y haga clic en **Submit**.

NOTA

Esta función solo se puede habilitar para oyentes HTTPS o HTTP.

### Desactivación de la función

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Summary**, haga clic en **Edit** en la parte superior derecha.
7. En el cuadro de diálogo **Edit**, expanda **Advanced Settings** y deshabilite la función.
8. Haga clic en **OK**.

## 3.8 Política de seguridad de TLS

### Escenarios

Al agregar oyentes de HTTPS, puede seleccionar las políticas de seguridad adecuadas para mejorar la seguridad. Una política de seguridad es una combinación de protocolos TLS de diferentes versiones y conjuntos de cifrado compatibles.

- Balanceadores de carga dedicados: puede seleccionar la política de seguridad predeterminada o crear una política personalizada. Para obtener más información, véase **Creación de una política de seguridad personalizada**.
- Balanceadores de carga compartidos: puede seleccionar la política de seguridad predeterminada.

NOTA

Las políticas de seguridad personalizadas solo se pueden crear en CN-Hong Kong, AP-Bangkok y AP-Singapore.

### Adición de una política de seguridad

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. En **Listeners**, haga clic en **Add Listener**.
6. En el cuadro de diálogo **Add Listener**, establezca **Frontend Protocol** en **HTTPS**.
7. Expanda **Advanced Settings** y seleccione una política de seguridad.

   **Tabla 3-13** muestra las políticas de seguridad predeterminadas. Seleccione una política de seguridad predeterminada o cree una política de seguridad personalizada haciendo referencia a **Creación de una política de seguridad personalizada**.

**Tabla 3-13** Políticas de seguridad predeterminadas

| Políticas de seguridad | Descripción | Versiones de TLS | Suites de cifrado |
|---|---|---|---|
| TLS-1-0 | TLS 1.0, TLS 1.1 y TLS 1.2 y suites de cifrado compatibles (alta compatibilidad y seguridad moderada) | TLS 1.2<br>TLS 1.1<br>TLS 1.0 | ● ECDHE-RSA-AES256-GCM-SHA384<br>● ECDHE-RSA-AES128-GCM-SHA256<br>● ECDHE-ECDSA-AES256-GCM-SHA384<br>● ECDHE-ECDSA-AES128-GCM-SHA256<br>● AES128-GCM-SHA256<br>● AES256-GCM-SHA384<br>● ECDHE-ECDSA-AES128-SHA256<br>● ECDHE-RSA-AES128-SHA256<br>● AES128-SHA256<br>● AES256-SHA256<br>● ECDHE-ECDSA-AES256-SHA384<br>● ECDHE-RSA-AES256-SHA384<br>● ECDHE-ECDSA-AES128-SHA<br>● ECDHE-RSA-AES128-SHA<br>● ECDHE-RSA-AES256-SHA<br>● ECDHE-ECDSA-AES256-SHA<br>● AES128-SHA<br>● AES256-SHA |
| TLS-1-1 | TLS 1.1 y TLS 1.2 y suites de cifrado compatibles (compatibilidad moderada y seguridad moderada) | TLS 1.2<br>TLS 1.1 | |
| TLS-1-2 | TLS 1.2 y suites de cifrado compatibles (compatibilidad moderada y alta seguridad) | TLS 1.2 | |

| Políticas de seguridad | Descripción | Versiones de TLS | Suites de cifrado |
| --- | --- | --- | --- |
| TLS-1-2-Strict | Estricto TLS 1.2 y suites de cifrado compatibles (baja compatibilidad y seguridad ultraalta) | TLS 1.2 | • ECDHE-RSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES256-GCM-SHA384<br>• ECDHE-ECDSA-AES128-GCM-SHA256<br>• AES128-GCM-SHA256<br>• AES256-GCM-SHA384<br>• ECDHE-ECDSA-AES128-SHA256<br>• ECDHE-RSA-AES128-SHA256<br>• AES128-SHA256<br>• AES256-SHA256<br>• ECDHE-ECDSA-AES256-SHA384<br>• ECDHE-RSA-AES256-SHA384 |

| Políticas de seguridad | Descripción | Versiones de TLS | Suites de cifrado |
|---|---|---|---|
| TLS-1-0-WITH-1-3 (para balanceadores de carga dedicados) | TLS 1.0 y posteriores, y suites de cifrado compatibles (compatibilidad ultraalta y baja seguridad) | TLS 1.3<br>TLS 1.2<br>TLS 1.1<br>TLS 1.0 | ● ECDHE-RSA-AES256-GCM-SHA384<br>● ECDHE-RSA-AES128-GCM-SHA256<br>● ECDHE-ECDSA-AES256-GCM-SHA384<br>● ECDHE-ECDSA-AES128-GCM-SHA256<br>● AES128-GCM-SHA256<br>● AES256-GCM-SHA384<br>● ECDHE-ECDSA-AES128-SHA256<br>● ECDHE-RSA-AES128-SHA256<br>● AES128-SHA256<br>● AES256-SHA256<br>● ECDHE-ECDSA-AES256-SHA384<br>● ECDHE-RSA-AES256-SHA384<br>● ECDHE-ECDSA-AES128-SHA<br>● ECDHE-RSA-AES128-SHA<br>● ECDHE-RSA-AES256-SHA<br>● ECDHE-ECDSA-AES256-SHA<br>● AES128-SHA<br>● AES256-SHA<br>● TLS_AES_128_GCM_SHA256<br>● TLS_AES_256_GCM_SHA384<br>● TLS_CHACHA20_POLY1305_SHA256<br>● TLS_AES_128_CCM_SHA256<br>● TLS_AES_128_CCM_8_SHA256 |

| Políticas de seguridad | Descripción | Versiones de TLS | Suites de cifrado |
|---|---|---|---|
| TLS-1-2-FS-WITH-1-3 (para balanceadores de carga dedicados) | TLS 1.2 y posteriores, y suites de cifrado de secreto hacia adelante compatibles (alta compatibilidad y seguridad ultraalta) | TLS 1.3<br>TLS 1.2 | • ECDHE-RSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES256-GCM-SHA384<br>• ECDHE-ECDSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES128-SHA256<br>• ECDHE-RSA-AES128-SHA256<br>• ECDHE-ECDSA-AES256-SHA384<br>• ECDHE-RSA-AES256-SHA384<br>• TLS_AES_128_GCM_SHA256<br>• TLS_AES_256_GCM_SHA384<br>• TLS_CHACHA20_POLY1305_SHA256<br>• TLS_AES_128_CCM_SHA256<br>• TLS_AES_128_CCM_8_SHA256 |
| TLS-1-2-FS (para balanceadores de carga dedicados) | TLS 1.2 y suites de cifrado de secreto directo compatibles (compatibilidad moderada y seguridad ultraalta) | TLS 1.2 | • ECDHE-RSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES256-GCM-SHA384<br>• ECDHE-ECDSA-AES128-GCM-SHA256<br>• ECDHE-ECDSA-AES128-SHA256<br>• ECDHE-RSA-AES128-SHA256<br>• ECDHE-ECDSA-AES256-SHA384<br>• ECDHE-RSA-AES256-SHA384 |

| Políticas de seguridad | Descripción | Versiones de TLS | Suites de cifrado |
| --- | --- | --- | --- |
| tls-1-2-strict-no-cbc (balanceadores de carga dedicados) | TLS 1.2 y conjuntos de encriptación compatibles que excluyen el algoritmo de encriptación CBC (baja compatibilidad y seguridad ultraalta) | TLS 1.2 | • ECDHE-ECDSA-AES256-GCM-SHA384<br>• ECDHE-ECDSA-AES128-GCM-SHA256<br>• ECDHE-RSA-AES256-GCM-SHA384<br>• ECDHE-RSA-AES128-GCM-SHA256 |

NOTA

- TLS-1-0-WITH-1-3, TLS-1-2-FS-WITH-1-3, TLS-1-2-FS, hybrid-policy-1-0 y tls-1-2-strict-no-cbc solo están disponibles para balanceadores de carga dedicados.
- La última versión de TLS soportada por balanceadores de carga dedicados es TLS 1.3, mientras que la última versión soportada por balanceadores de carga compartidos es TLS 1.2.
- Esta tabla enumera los conjuntos de cifrado soportados por ELB. En general, los clientes también admiten múltiples suites de cifrado. En uso real, se utiliza la intersección de los conjuntos de cifrado soportados por ELB y aquellos soportados por los clientes, y los conjuntos de cifrado soportados por ELB tienen prioridad.

8. Haga clic en **OK**.

## Diferencias entre las políticas de seguridad

**Tabla 3-14** Diferencias entre las políticas de seguridad

| Política de seguridad | TLS-1-0 | TLS-1-1 | TLS-1-2 | TLS-1-2-Strict | TLS-1-0-WITH-1-3 | TLS-1-2-FS-WITH-1-3 | TLS-1-2-FS |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Versiones de TLS | | | | | | | |
| TLS 1.3 | - | - | - | - | √ | √ | √ |
| TLS 1.2 | √ | √ | √ | √ | √ | √ | √ |
| TLS 1.1 | √ | √ | - | - | √ | - | - |
| TLS 1.0 | √ | - | - | - | √ | - | - |
| Cipher suite | | | | | | | |
| EDHE-RSA-AES128-GCM-SHA256 | √ | √ | √ | √ | - | - | - |

| Política de seguridad | TLS-1-0 | TLS-1-1 | TLS-1-2 | TLS-1-2-Strict | TLS-1-0-WITH-1-3 | TLS-1-2-FS-WITH-1-3 | TLS-1-2-FS |
|---|---|---|---|---|---|---|---|
| ECDHE-RSA-AES256-GCM-SHA384 | √ | √ | √ | √ | √ | √ | √ |
| ECDHE-RSA-AES128-SHA256 | √ | √ | √ | √ | √ | √ | √ |
| ECDHE-RSA-AES256-SHA384 | √ | √ | √ | √ | √ | √ | √ |
| AES128-GCM-SHA256 | √ | √ | √ | √ | √ | - | - |
| AES256-GCM-SHA384 | √ | √ | √ | √ | √ | - | - |
| AES128-SHA256 | √ | √ | √ | √ | √ | - | - |
| AES256-SHA256 | √ | √ | √ | √ | √ | - | - |
| ECDHE-RSA-AES128-SHA | √ | √ | √ | - | √ | - | - |
| ECDHE-RSA-AES256-SHA | √ | √ | √ | - | √ | - | - |
| AES128-SHA | √ | √ | √ | - | √ | - | - |
| AES256-SHA | √ | √ | √ | - | √ | - | - |
| ECDHE-ECDSA-AES128-GCM-SHA256 | √ | √ | √ | √ | √ | √ | √ |
| ECDHE-ECDSA-AES128-SHA256 | √ | √ | √ | √ | √ | √ | √ |
| ECDHE-ECDSA-AES128-SHA | √ | √ | √ | - | √ | - | - |
| ECDHE-ECDSA-AES256-GCM-SHA384 | √ | √ | √ | √ | √ | √ | √ |
| ECDHE-ECDSA-AES256-SHA384 | √ | √ | √ | √ | √ | √ | √ |
| ECDHE-ECDSA-AES256-SHA | √ | √ | √ | - | √ | - | - |
| ECDHE-RSA-AES128-GCM-SHA256 | - | - | - | - | √ | √ | √ |

| Política de seguridad | TLS-1-0 | TLS-1-1 | TLS-1-2 | TLS-1-2-Strict | TLS-1-0-WITH-1-3 | TLS-1-2-FS-WITH-1-3 | TLS-1-2-FS |
|---|---|---|---|---|---|---|---|
| TLS_AES_256_GCM_SHA384 | - | - | - | - | √ | √ | √ |
| TLS_CHACHA20_POLY1305_SHA256 | - | - | - | - | √ | √ | √ |
| TLS_AES_128_GCM_SHA256 | - | - | - | - | √ | √ | √ |
| TLS_AES_128_CCM_8_SHA256 | - | - | - | - | √ | √ | √ |
| TLS_AES_128_CCM_SHA256 | - | - | - | - | √ | √ | √ |

## Creación de una política de seguridad personalizada

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **TLS Security Policies**.
5. En la página mostrada, haga clic en **Create Custom Security Policy** en la esquina superior derecha.
6. Configura los parámetros basados en **Tabla 3-15**.

**Tabla 3-15** Parámetros de política de seguridad personalizados

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Name | Especifica el nombre de la política de seguridad personalizada. | tls-test |
| TLS Version | Especifica la versión de TLS admitida por la política de seguridad personalizada. Puede seleccionar varias versiones:<br>● TLS 1.0<br>● TLS 1.1<br>● TLS 1.2<br>● TLS 1.3 | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Cipher Suite | Especifica los conjuntos de cifrado que coinciden con las versiones de TLS seleccionadas. | - |
| Description | Proporciona información adicional acerca de la política de seguridad personalizada. | - |

7. Haga clic en **OK**.

## Modificación de una política de seguridad personalizada

Puede modificar una política de seguridad personalizada según lo necesite.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **TLS Security Policies**.
5. En la página **TLS Security Policies**, haga clic en **Custom Security Policies**, busque la política de seguridad personalizada y haga clic en **Modify** en la columna **Operation**.
6. En el cuadro de diálogo que se muestra, modifique la política de seguridad personalizada como se describe en **Tabla 3-15**.
7. Haga clic en **OK**.

## Eliminación de una política de seguridad personalizada

Puede eliminar una política de seguridad personalizada según lo necesite.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **TLS Security Policies**.
5. En la página **TLS Security Policies**, haga clic en **Custom Security Policies**, busque la política de seguridad personalizada y haga clic en **Delete** en la columna **Operation**.
6. Haga clic en **Yes**.

## Cambio de una política de seguridad

Cuando cambie una política de seguridad, asegúrese de que el grupo de seguridad que contiene servidores backend permita el tráfico de 100.125.0.0/16 a servidores backend y permita paquetes ICMP para comprobaciones de estado UDP. De lo contrario, los servidores backend se considerarán no saludables y el enrutamiento se verá afectado.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Summary**, haga clic en **Edit** en la parte superior derecha.
7. En el cuadro de diálogo **Modify Listener**, expanda **Advanced Settings** y cambie la política de seguridad.
8. Haga clic en **OK**.

# 3.9 Certificado de SNI (para oyentes de HTTPS)

## Escenarios

Si tiene una aplicación a la que se puede acceder a través de varios nombres de dominio y cada nombre de dominio utiliza un certificado diferente, puede habilitar la indicación de nombre de servidor (SNI) cuando agrega un oyente HTTPS.

SNI, una extensión de Transport Layer Security (TLS), permite a un servidor presentar varios certificados en la misma dirección IP y número de puerto. SNI permite al cliente indicar el nombre de dominio del sitio web mientras envía una solicitud de protocolo de enlace SSL. Una vez que recibe la solicitud, el balanceador de carga consulta el certificado correcto basado en el nombre de host o el nombre de dominio y devuelve el certificado al cliente. Si no se encuentra ningún certificado, el balanceador de carga devolverá el certificado predeterminado.

Puede habilitar el SNI solo cuando agrega oyentes de HTTPS. Los balanceadores de carga pueden tener varios certificados SNI enlazados.

## Restricciones

Un oyente de HTTPS puede tener hasta 30 certificados SNI. Todos los certificados pueden tener hasta 30 nombres de dominio.

NOTA

Los oyentes de un balanceador de carga dedicado pueden tener hasta 50 certificados SNI. Puede enviar un ticket de servicio para aumentar la cuota.

## Requisitos previos

- Ha agregado un oyente HTTPS al balanceador de carga realizando las operaciones en **Adición de un oyente de HTTPS**.
- Ha creado un certificado SNI realizando las operaciones de **Adición de un certificado**.

NOTA

- Debe especificar un nombre de dominio para un certificado SNI. El nombre de dominio debe ser el mismo que el del certificado.
- Un nombre de dominio puede ser utilizado tanto por un certificado ECC como por un certificado RSA. Si hay dos certificados SNI que utilizan el mismo nombre de dominio, el certificado ECC se muestra preferentemente.
- Los nombres de dominio de un certificado SNI coinciden de la siguiente manera:

  Si el nombre de dominio del certificado es *.test.com, a.test.com y b.test.com son compatibles, y a.b.test.com y c.d.test.com no son compatibles.

  El nombre de dominio con el sufijo más largo coincide: Si un certificado contiene *.b.test.com y *.test.com, a.b.test.com coincide preferentemente con *.b.test.com.
- Si un certificado ha caducado, debe reemplazarlo o eliminarlo manualmente siguiendo las instrucciones en **Vinculación de un oyente y sustitución del certificado enlazado a un oyente**.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En la página de ficha **Summary**, haga clic en **Edit** en la parte superior derecha.
7. Habilite SNI y seleccione un certificado de SNI.
8. Haga clic en **OK**.

# 4 Grupo de servidores backend

## 4.1 Descripción general

### Introducción

Un grupo de servidores backend es una colección lógica de uno o más servidores backend para recibir solicitudes simultáneas masivas al mismo tiempo. Un servidor backend puede ser un ECS, un BMS, una interfaz de red suplementaria o una dirección IP.

El siguiente proceso describe cómo un grupo de servidores backend reenvía el tráfico:

1. Un cliente envía una solicitud a su aplicación. Los oyentes agregados al balanceador de carga utilizan los protocolos y puertos que ha configurado reenvían la solicitud al grupo de servidores backend asociado.
2. Los servidores backend de buen estado del grupo de servidores backend reciben la solicitud basada en el algoritmo de balanceo de carga, manejan la solicitud y devuelven un resultado al cliente.
3. De esta manera, las solicitudes simultáneas masivas se pueden procesar al mismo tiempo, mejorando la disponibilidad de sus aplicaciones.

Para los balanceadores de carga dedicados, el tipo de grupo de servidores backend puede ser **Hybrid** o **IP as a backend server**. Puede agregar un ECS, un BMS, una interfaz de red suplementaria o una dirección IP a un grupo de servidores backend híbrido. Si establece el tipo en **IP as a backend server**, solo puede agregar direcciones IP como servidores backend.

Los balanceadores de carga compartidos solo tienen un tipo de grupo de servidores backend, donde solo se pueden agregar servidores en la nube.

**Figura 4-1** muestra la arquitectura de diferentes tipos de grupos de servidores backend.

**Figura 4-1** Arquitectura de grupo de servidores backend

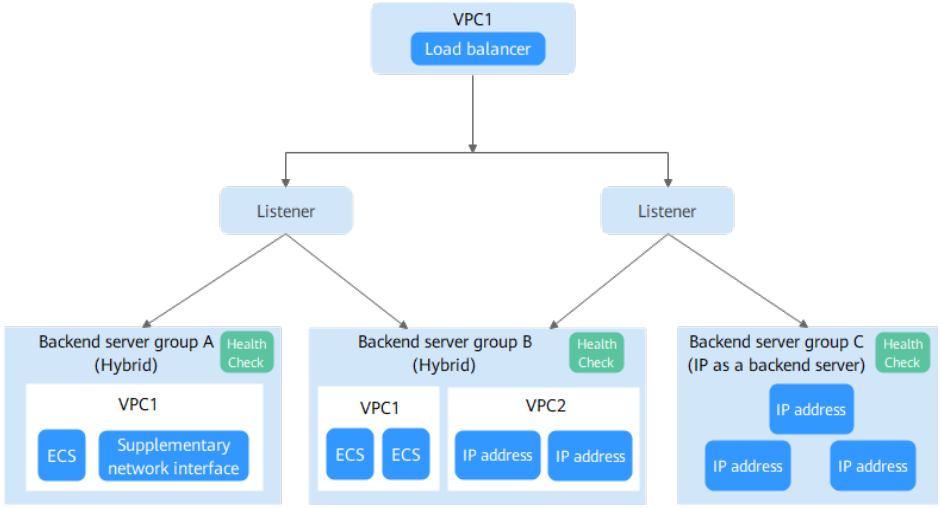



**Tabla 4-1** Tipos de grupo de servidores backend

| Tipo de grupo de servidores backend | Tipo de servidor backend | Ejemplo | Referencia |
|---|---|---|---|
| Híbrido | • ECS, BMS o interfaces de red suplementarias que están en la misma VPC que el balanceador de carga<br>• Servidores en la nube en otras VPC o servidores locales si IP como backend está habilitado para el balanceador de carga | Como se muestra en **Figura 4-1**:<br>• En el grupo de servidores backend A, puede agregar servidores o interfaces de red suplementarias en VPC1.<br>• En el grupo B de servidores backend, puede agregar direcciones IP en VPC2 como servidores backend. | • **Adición de servidores backend**<br>• **Adición de interfaces de red suplementarias**<br>• **Adición de direcciones IP como servidores backend** |
| IP como servidor backend | Servidores en la nube en otras VPC o servidores locales si IP como backend está habilitado para el balanceador de carga | Como se muestra en **Figura 4-1**, las direcciones IP se pueden agregar al grupo C de servidores backend como servidores backend. | **Adición de direcciones IP como servidores backend** |

## Ventajas

Los grupos de servidores backend pueden aportar las siguientes ventajas:

- **Reduced costs and easier management**: Puede agregar o quitar servidores backend a medida que el tráfico cambie con el tiempo. Esto puede ayudar a evitar la baja utilización de recursos y facilita la gestión de servidores backend.
- **Higher reliability**: El tráfico se enruta solo a servidores backend sanos en el grupo de servidores backend.

## Funciones principales

Puede configurar las funciones clave de **Tabla 4-2** para cada grupo de servidores backend para garantizar la estabilidad del servicio.

**Tabla 4-2** Funciones principales

| Función clave | Descripción | Detalle |
| --- | --- | --- |
| Comprobación de estado | Especifica si se activa la opción de comprobación de estado. Las comprobaciones de estado determinan si los servidores backend están en buen estado.<br>Si se detecta que un servidor backend no está sano, no recibirá solicitudes del balanceador de carga asociado, lo que mejorará la confiabilidad del servicio. | **Comprobación de estado** |
| Algoritmo de balanceo de carga | El balanceador de carga distribuye el tráfico basado en el algoritmo de balanceo de carga que ha configurado para el grupo de servidores backend. | **Algoritmos de balanceo de carga** |
| Sesión adhesiva | Especifica si se activa la opción de sesión adhesiva. Si habilita esta opción, todas las solicitudes de un cliente durante una sesión se envían al mismo servidor backend. | **Sesión adhesiva** |

| Función clave | Descripción | Detalle |
| --- | --- | --- |
| Inicio lento | Especifica si se habilitará el inicio lento. Después de habilitarlo, el balanceador de carga aumenta linealmente la proporción de solicitudes a los servidores backend en este modo.<br>Cuando transcurre la duración de inicio lento, el balanceador de carga envía una parte completa de las solicitudes a los servidores backend y sale del modo de inicio lento.<br>**NOTA**<br>El inicio lento solo está disponible para los grupos de servidores HTTP y HTTPS backend de balanceadores de carga dedicados. | **Inicio lento (balanceadores de carga dedicados)** |

## Precauciones para crear un grupo de servidores backend

El protocolo backend del nuevo grupo de servidores backend debe coincidir con el protocolo frontend del oyente como se describe en **Tabla 4-3**.

Puede crear un grupo de servidores backend haciendo referencia a **Tabla 4-4**.

**Tabla 4-3** El protocolo frontend y backend

| Protocolo frontend | Protocolo backend |
| --- | --- |
| TCP | TCP |
| UDP | ● UDP<br>● QUIC |
| HTTP | HTTP |
| HTTPS | ● HTTP<br>● HTTPS |

**Tabla 4-4** Creación de un grupo de servidores backend

| Tipo de balanceador de carga | Referencia |
| --- | --- |
| Dedicado | **Creación de un grupo de servidores backend (balanceadores de carga dedicados)** |
| Compartido | **Creación de un grupo de servidores backend (balanceadores de carga compartidos)** |

# 4.2 Características principales

## 4.2.1 Comprobación de estado

ELB envía periódicamente solicitudes a los servidores backend para comprobar si pueden procesar solicitudes. Este proceso se llama comprobación de estado.

Si se detecta un servidor backend que no está sano, el balanceador de carga detendrá las solicitudes de enrutamiento a él. Después de que el servidor backend se recupere, el balanceador de carga reanudará las solicitudes de enrutamiento a él.

Si los servidores backend tienen que manejar un gran número de solicitudes, las comprobaciones de estado frecuentes pueden sobrecargar los servidores backend y hacer que respondan lentamente. Para solucionar este problema, puede prolongar el intervalo de comprobación de estado o utilizar TCP o UDP en lugar de HTTP. También puede desactivar la comprobación de estado. Si decide desactivar la comprobación de estado, es posible que las solicitudes se enruten a servidores que no estén sanos y que se produzcan interrupciones del servicio.

### Protocolo de comprobación de estado

Puede configurar las comprobaciones de estado al configurar grupos de servidores backend. En general, puede utilizar la configuración predeterminada o seleccionar un protocolo de comprobación de estado diferente según lo necesite.

Si desea modificar la configuración de la comprobación de estado, consulte los detalles de **Modificación de la configuración de comprobación de estado**.

Seleccione un protocolo de comprobación de estado que coincida con el protocolo de backend como se describe en **Tabla 4-5** y **Tabla 4-6**.

**Tabla 4-5** El protocolo de backend y los protocolos de comprobación de estado (balanceadores de carga dedicados)

| Protocolo backend | Protocolo de comprobación de estado |
|---|---|
| TCP | TCP, UDP, HTTP o HTTPS |
| UDP | UDP |
| QUIC | UDP |
| HTTP | TCP, HTTP, HTTPS |
| HTTPS | TCP, HTTP, HTTPS |

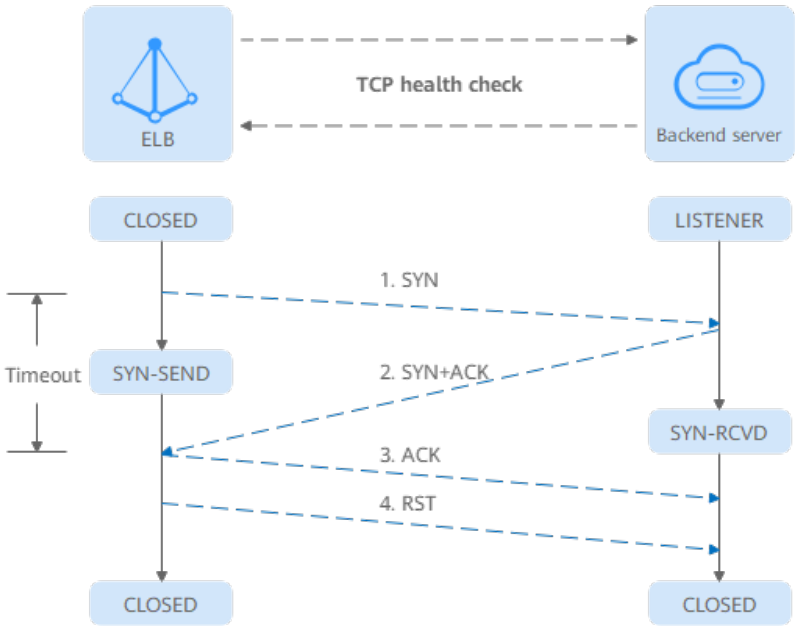
**Tabla 4-6** Protocolo de back-end y protocolos de comprobación de estado (balanceadores de carga compartidos)

| Protocolo backend | Protocolo de comprobación de estado |
| --- | --- |
| TCP | TCP o HTTP |
| UDP | UDP |
| HTTP | TCP o HTTP |
| HTTPS | TCP o HTTP |

## Comprobación de estado de TCP

Para los protocolos de backend TCP, HTTP y HTTPS, puede usar TCP para iniciar acuerdos de enlace de tres vías para obtener los estados de los servidores de backend.

**Figura 4-2** Comprobación de estado de TCP




El proceso de comprobación de estado de TCP es el siguiente:

1. El balanceador de carga envía un paquete TCP SYN al servidor backend (en el formato de *Private IP address*}:{*Health check port*).
2. El servidor backend devuelve un paquete SYN-ACK.
   - Si el balanceador de carga no recibe el paquete SYN-ACK dentro de la duración del tiempo de espera, declara que el servidor backend no está sano y envía un paquete RST al servidor backend para terminar la conexión de TCP.
   - Si el balanceador de carga recibe el paquete SYN-ACK desde el servidor backend dentro de la duración del tiempo de espera, envía un paquete ACK al servidor backend y declara que el servidor backend está en buen estado. Después de eso, el balanceador de carga envía un paquete RST al servidor back-end para terminar la conexión de TCP.

**AVISO**

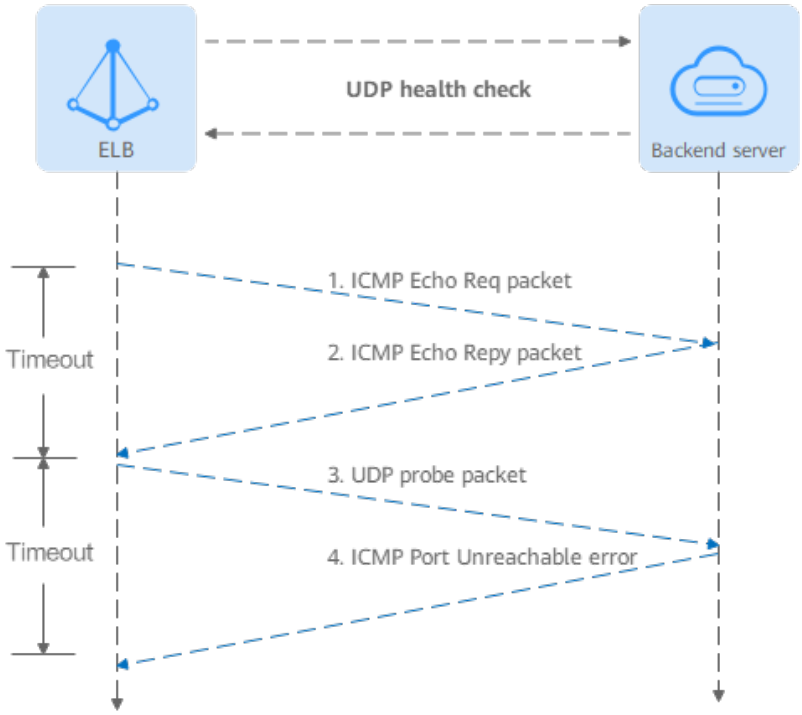
Después de un protocolo de enlace de tres vías TCP exitoso, se enviará un paquete RST para cerrar la conexión TCP. La aplicación en el servidor backend puede considerar este paquete como un error de conexión y responder con un mensaje, por ejemplo, "Connection reset by peer". Para evitar este problema, realice cualquiera de las siguientes acciones:

- Use **Comprobación de estado de HTTP**.
- Haga que el servidor backend ignore el error de conexión.

## Comprobación de estado de UDP

Para el protocolo backend de UDP, ELB envía paquetes de sondeo ICMP y UDP a los servidores backend para comprobar su estado.

**Figura 4-3** Comprobación de estado de UDP




El proceso de comprobación de estado de UDP es el siguiente:

1. El balanceador de carga envía un paquete de ICMP Echo Request al servidor backend.
   - Si el balanceador de carga no recibe un paquete ICMP Echo Reply dentro de la duración del tiempo de espera de comprobación de estado, el servidor backend se declara no saludable.
   - Si el balanceador de carga recibe un paquete ICMP Echo Reply dentro del período de tiempo de espera, envía un paquete de sondeo UDP al servidor backend.
2. Si el balanceador de carga no recibe un error ICMP Port Unreachable dentro de la duración del tiempo de espera de comprobación de estado, declara que el servidor backend está en buen estado. Si el balanceador de carga recibe un error ICMP Port Unreachable, el servidor backend se declara insalubre.

## Comprobación de estado de HTTP

También puede configurar las comprobaciones de estado de HTTP para obtener los estados del servidor con las solicitudes HTTP GET si selecciona TCP, HTTP o HTTPS como protocolo backend. **Figura 4-4 Figura 4-4** muestra cómo funciona una comprobación de estado HTTP.

**Figura 4-4** Comprobación de estado de HTTP


El proceso de comprobación de estado HTTPS es el siguiente:

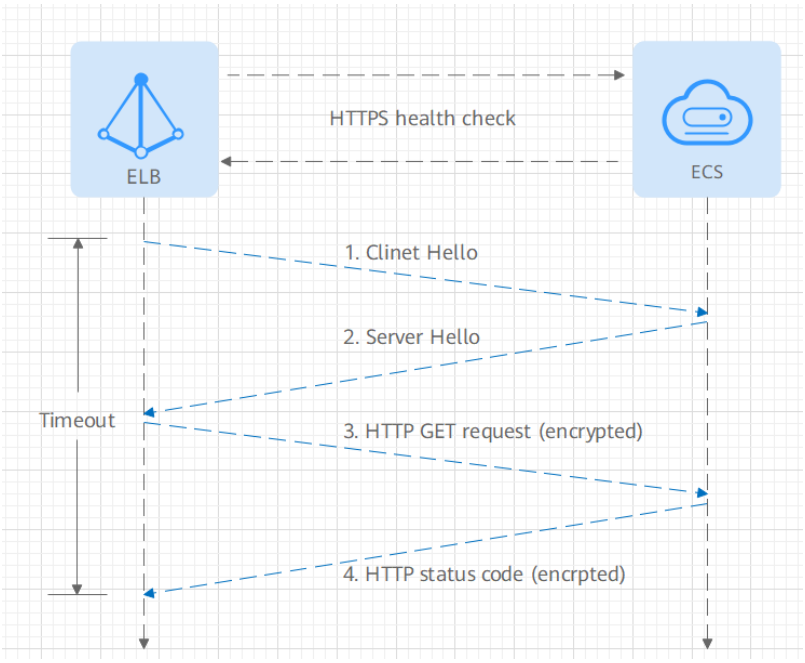
1. El balanceador de carga envía una solicitud de HTTP GET al servidor backend (en formato de *{Private IP address}*:*{Health check port}*/*{Health check path}*). (Puede especificar un nombre de dominio al configurar una comprobación de estado.)
2. El servidor backend devuelve un código de estado HTTP a ELB.
   - Si el balanceador de carga recibe el código de estado dentro de la duración del tiempo de espera de comprobación de estado, compara el código de estado con el preestablecido. Si los códigos de estado son los mismos, el servidor backend se declara en buen estado.
   - Si el balanceador de carga no recibe ninguna respuesta del servidor backend dentro de la duración del tiempo de espera de comprobación de estado, declara que el servidor backend no está sano.

## Comprobación de estado de HTTPS

Para los protocolos de backend TCP, HTTP y HTTPS, puede usar HTTPS para establecer una conexión SSL a través de TLS para obtener los estados de los servidores de backend. **Figura 4-5** muestra cómo funciona una comprobación de estado HTTPS.

**Figura 4-5** Comprobación de estado de HTTPS




El proceso de comprobación de estado HTTPS es el siguiente:

1. El balanceador de carga envía un paquete de Client Hello para establecer una conexión SSL con el servidor backend.
2. Después de recibir el paquete Server Hello desde el servidor back-end, el balanceador de carga envía una solicitud de HTTP GET encriptada al servidor back-end (en el formato de *{Dirección IP privada}*:*{Puerto de comprobación de salud}*/*{Ruta de comprobación de salud}*). (Puede especificar un nombre de dominio al configurar una comprobación de estado.)
3. El servidor backend devuelve un código de estado HTTP al balanceador de carga.
   - Si el balanceador de carga recibe el código de estado dentro de la duración del tiempo de espera de comprobación de estado, compara el código de estado con el preestablecido. Si los códigos de estado son los mismos, el servidor backend se declara en buen estado.
   - Si el balanceador de carga no recibe ninguna respuesta del servidor backend dentro de la duración del tiempo de espera de comprobación de estado, declara que el servidor backend no está sano.

## Ventana de tiempo de comprobación de estado

Las comprobaciones de estado mejoran considerablemente la disponibilidad del servicio. Sin embargo, si los controles de estado son demasiado frecuentes, la disponibilidad del servicio se verá comprometida. Para evitar el impacto, ELB declara un servidor backend en buen estado o en mal estado después de varias comprobaciones de estado consecutivas.

La ventana de tiempo de comprobación de estado viene determinada por los factores de **Tabla 4-7**:

**Tabla 4-7** Factores que afectan a la ventana de tiempo de comprobación de estado

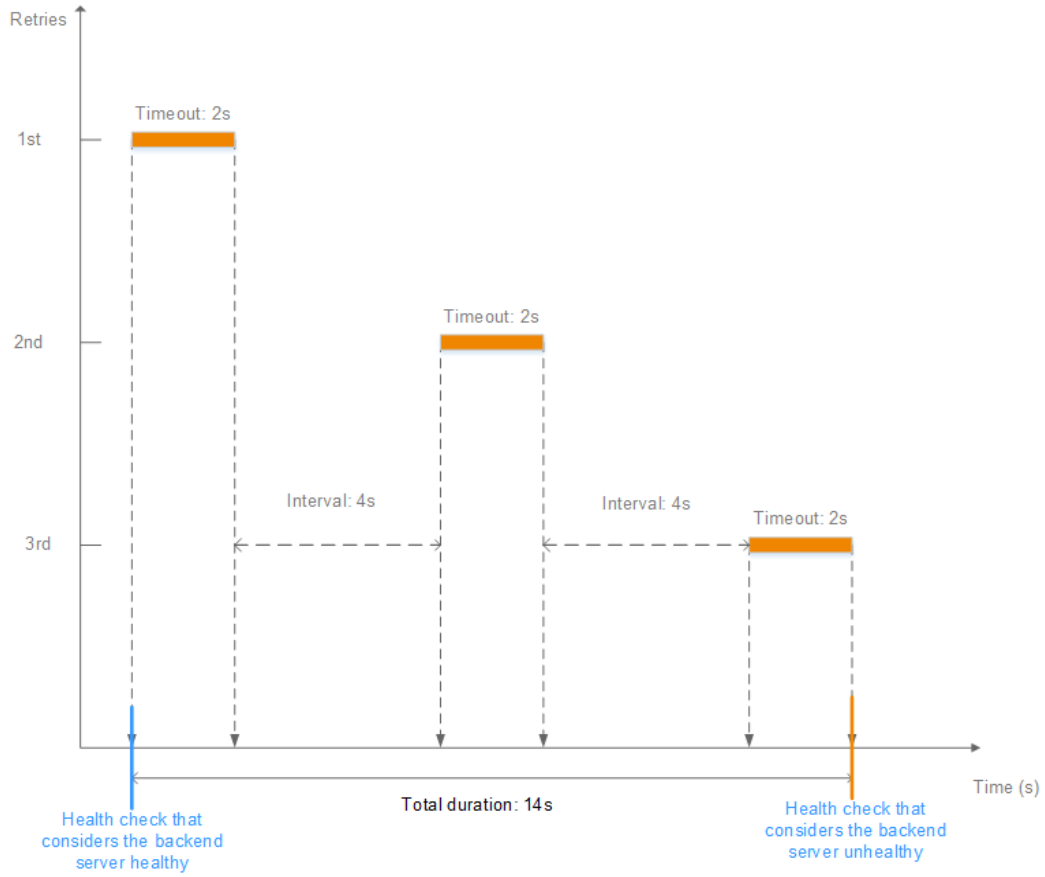
| Factor | Descripción |
| --- | --- |
| Intervalo de verificación | Con qué frecuencia se realizan comprobación de salud. |
| Duración del tiempo de espera | Cuánto tiempo espera el balanceador de carga para la respuesta del servidor backend. |
| Umbral de comprobación de estado | Número de comprobaciones de estado exitosas o fallidas consecutivas requeridas para determinar si el servidor backend está sano o no. |

La siguiente es una fórmula para calcular la ventana de tiempo de comprobación de estado:

- Ventana de tiempo para que un servidor backend se detecte sano = Duración de tiempo de espera x umbral saludable + Intervalo x (umbral saludable – 1)
- Ventana de tiempo para que un servidor backend se detecte insalubre = Duración de tiempo de espera x umbral insalubre + Intervalo x (umbral insalubre – 1)

Como se muestra en **Figura 4-6**, si el intervalo de comprobación de salud es 4s, la duración del tiempo de espera de comprobación de salud es 2s, y el umbral de insalubridad es 3, la ventana de tiempo para que un servidor backend se considere insalubridad se calcula de la siguiente manera: 2 x 3 + 4 x (3 – 1) = 14s.

**Figura 4-6** Duración del tiempo de espera de la comprobación de estado



### Rectificación de un servidor backend poco saludable

Si se detecta un servidor backend que no está sano, consulte **¿Cómo soluciono problemas de un servidor backend insalubre?**

## 4.2.2 Algoritmos de balanceo de carga

Los balanceadores de carga reciben solicitudes de clientes y las reenvían a servidores backend en una o más AZ. Cada balanceador de carga tiene al menos un oyente y un servidor backend. El algoritmo de balanceo de carga que seleccione al crear el grupo de servidores backend determina cómo se distribuyen las solicitudes.

### Algoritmos de balanceo de carga

Los balanceadores de carga dedicados admiten cuatro algoritmos de balanceo de carga: round robin ponderado, conexiones mínimas ponderadas, hash IP de origen e ID de conexión.

Los balanceadores de carga compartidos admiten round robin ponderado, conexiones menores ponderadas y hash IP de origen.

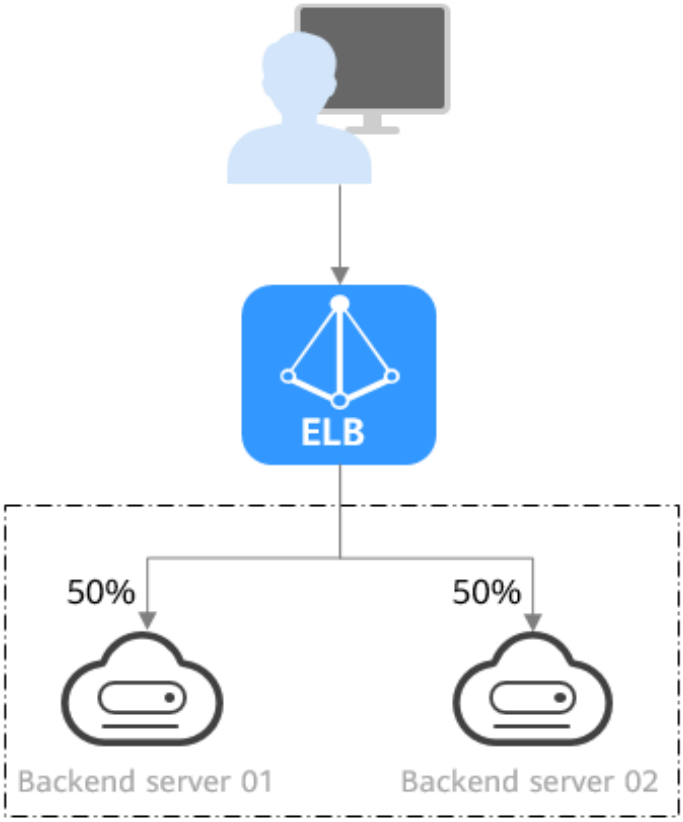
- Round robin ponderado: las solicitudes se enrutan a los servidores backend utilizando el algoritmo round robin. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.

  Este algoritmo se usa típicamente para conexiones cortas, tales como conexiones de HTTP.

  La **Figura 4-7** muestra un ejemplo de cómo se distribuyen las solicitudes usando el algoritmo round robin ponderado. Dos servidores backend están en la misma AZ y tienen el mismo peso, y cada servidor recibe la misma proporción de solicitudes.

**Figura 4-7** Distribución del tráfico utilizando el algoritmo de round robin ponderado



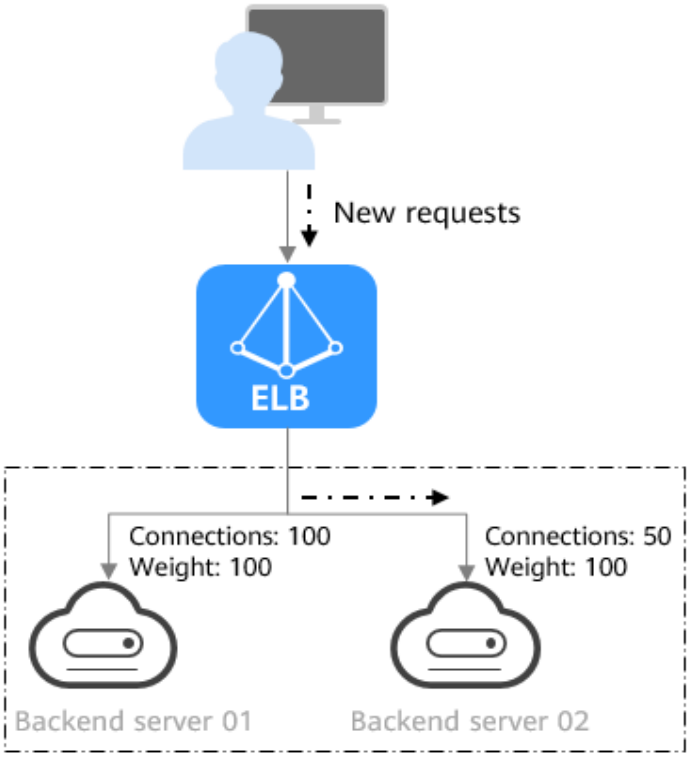

- Conexiones mínimas ponderadas: Además del peso asignado a cada servidor, también se tiene en cuenta el número de conexiones procesadas por cada servidor backend. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.

  Este algoritmo se utiliza a menudo para conexiones persistentes, como conexiones a una base de datos.

  La **Figura 4-8** muestra un ejemplo de cómo se distribuyen las solicitudes usando el algoritmo de conexiones mínimas ponderadas. Dos servidores de backend están en la misma AZ y tienen la misma ponderación, se han establecido 100 conexiones con el servidor backend 01, y se han conectado 50 conexiones con el servidor backend 02. Las nuevas peticiones se encaminan preferentemente al servidor de backend 02.

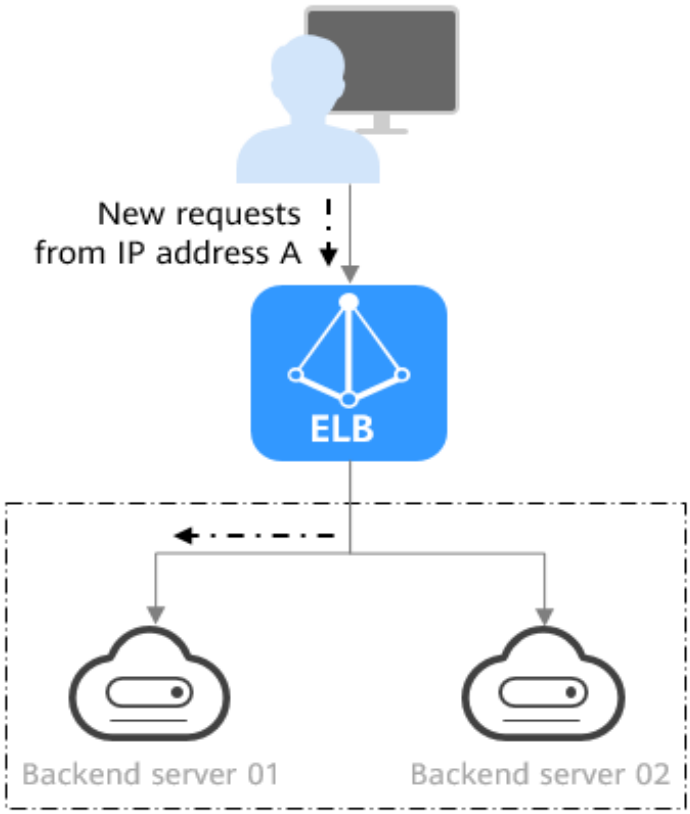
**Figura 4-8** Distribución del tráfico utilizando el algoritmo de conexiones mínimas ponderadas




- Source IP hash: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave hash única, y todos los servidores backend están numerados. La clave generada asigna el cliente a un servidor determinado. Esto permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que las solicitudes del mismo cliente se dirijan al mismo servidor que estaba usando anteriormente.

  **Figura 4-9** muestra un ejemplo de cómo se distribuyen las solicitudes usando el algoritmo hash IP de origen. Dos servidores backend están en la misma AZ y tienen la misma ponderación. Si el servidor backend 01 ha procesado una solicitud desde la dirección IP A, el balanceador de carga encaminará nuevas solicitudes desde la dirección IP A al servidor backend 01.

**Figura 4-9** Distribución del tráfico mediante el algoritmo de hash IP de origen




- ID de conexión: El ID de conexión en el paquete se calcula utilizando el algoritmo hash consistente para obtener un valor específico, y los servidores backend se numeran. El valor generado determina a qué servidor backend se enrutan las solicitudes. Esto permite que las solicitudes con diferentes ID de conexión se enruten a diferentes servidores backend y garantiza que las solicitudes con el mismo ID de conexión se enruten al mismo servidor backend.

  Este algoritmo se aplica a las solicitudes QUIC.

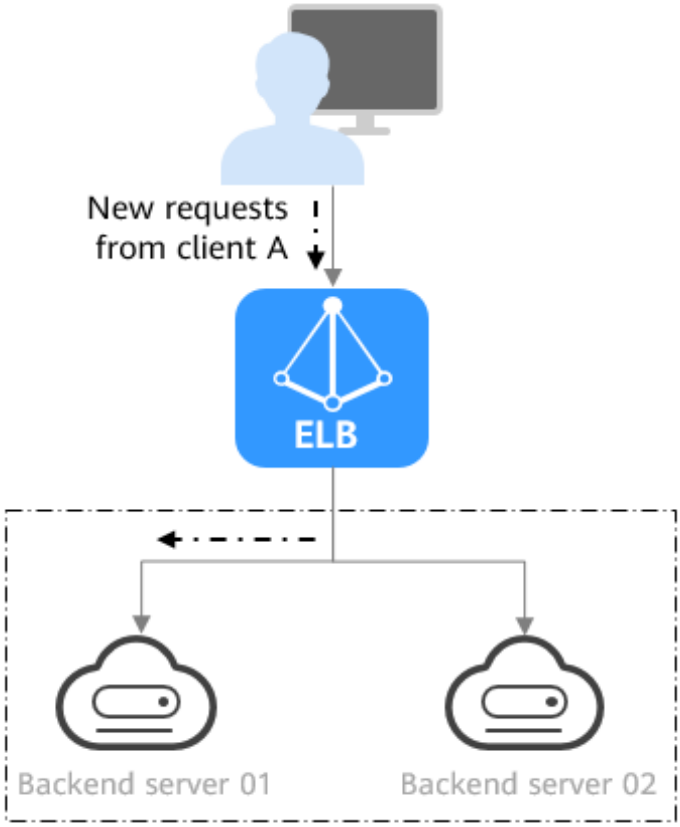
  NOTA

  Solo los balanceadores de carga dedicados soportan este algoritmo.

  La **Figura 4-10** muestra un ejemplo de cómo se distribuyen las solicitudes usando el algoritmo de ID de conexión. Dos servidores backend están en la misma AZ y tienen la misma ponderación. Si el servidor backend 01 ha procesado una solicitud del cliente A, el balanceador de carga encaminará nuevas solicitudes desde el cliente A al servidor backend 01.

**Figura 4-10** Distribución del tráfico mediante el algoritmo de ID de conexión




## 4.2.3 Sesión adhesiva

Las sesiones adhesivas garantizan que las solicitudes de un cliente siempre se enruten al mismo servidor backend antes de que transcurra una sesión.

Aquí hay un ejemplo que describe cómo funciona la sesión adhesiva. Suponga que ha iniciado sesión en un servidor. Después de un tiempo, envíe otra solicitud. Si las sesiones adhesivas no están habilitadas, es posible que la solicitud se enrute a otro servidor y se le pedirá que inicie sesión de nuevo. Si las sesiones adhesivas están habilitadas, todas sus solicitudes son procesadas por el mismo servidor, y no necesita iniciar sesión repetidamente.

### Diferencias entre las sesiones adhesivas en la capa 4 y la capa 7

La siguiente tabla describe las diferencias de las sesiones adhesivas en la Capa 4 en la Capa 7.

**Tabla 4-8** Comparación de sesión adhesiva

| Capa OSI | Protocolo de oyente | Tipo de sesión adhesiva | Duración de la pegajosidad | Escenarios donde las sesiones adhesivas se vuelven inválidas |
|---|---|---|---|---|
| Capa 4 | TCP o UDP | **Source IP address**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave de hash única, y todos los servidores backend están numerados. El sistema asigna el cliente a un servidor determinado basándose en la clave generada. Esto permite que las solicitudes de la misma dirección IP se reenvíen al mismo servidor backend. | • Predeterminado: 20 minutos<br>• Máximo: 60 minutos<br>• Rango: 1 minuto a 60 minutos | • Las direcciones IP de origen de los clientes cambian.<br>• Se ha alcanzado la duración de la pegajosidad de la sesión. |

| Capa OSI | Protocolo de oyente | Tipo de sesión adhesiva | Duración de la pegajosidad | Escenarios donde las sesiones adhesivas se vuelven inválidas |
|---|---|---|---|---|
| Capa 7 | HTTP o HTTPS | • **Load balancer cookie**: El balanceador de carga genera una cookie después de recibir una solicitud del cliente. Todas las solicitudes posteriores con la cookie se enrutan al mismo servidor backend.<br>• **Application cookie**: La aplicación desplegada en el servidor backend genera una cookie después de recibir la primera solicitud del cliente. Todas las solicitudes posteriores con la misma cookie se enrutan al mismo servidor backend. | • Predeterminado: 20 minutos<br>• Máximo: 1,440 minutos<br>• Rango: 1 minuto a 1,440 minutos | • Si las solicitudes enviadas por los clientes no contienen una cookie, las sesiones adhesivas no tendrán efecto.<br>• Las solicitudes de los clientes superan la duración de la sesión. |

NOTA

- Si establece **Load Balancing Algorithm** en **Source IP hash** no es necesario que active y configure **Sticky Session** manualmente. El hash IP de origen permite que las solicitudes del mismo cliente se dirijan al mismo servidor.
- Si establece **Load Balancing Algorithm** en **Weighted round robin** o **Weighted least connections**, debe habilitar y configurar manualmente **Sticky Session**.

## Restricciones y limitaciones

- Si utiliza **Cloud Connect connection**, **Direct Connect** o **VPN** para acceder a ELB, debe seleccionar **Source IP hash** como algoritmo de balanceo de carga y deshabilitar las sesiones adhesivas para ELB.
- Los balanceadores de carga dedicados admiten dos tipos de sesiones adhesivas: **Source IP address** y **Load balancer cookie**.

- Los balanceadores de carga compartidos admiten tres tipos de sesiones adhesivas: **Source IP address**, **Load balancer cookie** y **Application cookie**.

NOTA

- Para los oyentes HTTP y HTTPS, habilitar o deshabilitar sesiones adhesivas puede causar pocos segundos de interrupción del servicio.
- Si habilita las sesiones adhesivas, el tráfico a los servidores backend puede estar desequilibrado. Si esto sucede, deshabilite las sesiones adhesivas y compruebe las solicitudes recibidas por cada servidor backend.

## 4.2.4 Modo de reenvío (balanceadores de carga dedicados)

El balanceador de carga enruta el tráfico entre los servidores backend según el modo de reenvío. Hay dos opciones: **Load balancing** y **Active/Standby**.

NOTA

- Esta función solo está disponible para los grupos de servidores backend que están vinculados a balanceadores de carga dedicados.

**Tabla 4-9** Modos de reenvío

| Modo de reenvío | Descripción | Cuándo usarlo |
| --- | --- | --- |
| Equilibrio de carga | Puede agregar varios servidores backend a un grupo de servidores backend.<br>Y luego el balanceador de carga distribuye las solicitudes a través de estos servidores backend basados en el algoritmo de balanceo de carga configurado para este grupo de servidores backend. | Desea que su balanceador de carga reenvíe solicitudes basadas en las políticas de reenvío configuradas para el oyente. |
| Activo/en espera | Debe agregar dos servidores backend al grupo de servidores backend, uno que actúe como servidor activo y el otro como servidor en espera.<br>El reenvío activo/en espera requiere al menos un servidor backend en buen estado. El balanceador de carga enruta el tráfico al servidor activo si funciona normalmente. Si el servidor activo se vuelve insatisfactorio, el balanceador de carga enruta el tráfico al servidor en espera. | Necesita una mayor disponibilidad de servicio. |

## 4.2.5 Inicio lento (balanceadores de carga dedicados)

Si habilita el inicio lento, el balanceador de carga aumenta linealmente la proporción de solicitudes a los nuevos servidores backend agregados al grupo de servidores backend. Cuando transcurre la duración de inicio lento, el balanceador de carga envía una parte completa de las solicitudes a los servidores backend y sale del modo de inicio lento. Para

obtener más información acerca de cómo establecer ponderaciones para los servidores backend, consulte **Ponderación del servidor backend**.

El arranque lento da tiempo a las aplicaciones para calentar y responder a las solicitudes con un rendimiento óptimo.

NOTA

El inicio lento solo está disponible para los grupos de servidores HTTP y HTTPS backend de balanceadores de carga dedicados.

Los servidores backend saldrán de inicio lento en cualquiera de los siguientes casos:

- La duración de inicio lento transcurre.
- Los servidores de backend se vuelven insatisfactorios durante el inicio lento.

### Restricciones

- Se debe seleccionar round robin ponderado como algoritmo de balanceo de carga.
- El inicio lento solo tiene efecto para los nuevos servidores backend y no tiene efecto cuando el primer servidor backend se agrega a un grupo de servidores backend.
- Después de que transcurra la duración de inicio lento, los servidores backend no volverán a entrar en el modo de inicio lento.
- El inicio lento tiene efecto cuando la comprobación de estado está habilitada y los servidores backend se están ejecutando normalmente.
- Si la comprobación de estado está desactivada, el inicio lento entra en vigor inmediatamente.

## 4.3 Creación de un grupo de servidores backend (balanceadores de carga dedicados)

### Escenario

Para enrutar solicitudes, debe asociar al menos un grupo de servidores backend a cada oyente.

NOTA

Esta sección describe cómo crear un grupo de servidores backend para un balanceador de carga dedicado.

Puede crear un grupo de servidores backend para un balanceador de carga de cualquiera de las formas descritas en **Tabla 4-10**.

**Tabla 4-10** Creación de un grupo de servidores backend

| Escenario | Procedimiento |
| --- | --- |
| Creación de un grupo de servidores backend y asociarlo con un balanceador de carga | **Procedimiento** |

| Escenario | Procedimiento |
| --- | --- |
| Creación de un grupo de servidores backend al agregar un oyente | Puede agregar oyentes utilizando diferentes protocolos según sea necesario. Para obtener más información, véase **Descripción general**.<br>Las referencias son las siguientes:<br>● **Adición de un oyente de TCP**<br>● **Adición de un oyente de UDP**<br>● **Adición de un oyente de HTTP**<br>● **Adición de un oyente de HTTPS** |
| Cambio del grupo de servidores backend asociado al oyente | **Cambio de un grupo de servidores backend** |

## Restricciones

El protocolo backend del nuevo grupo de servidores backend debe coincidir con el protocolo frontend del oyente como se describe en **Tabla 4-11**.

**Tabla 4-11** El protocolo frontend y backend

| Protocolo frontend | Protocolo backend |
| --- | --- |
| TCP | TCP |
| UDP | ● UDP<br>● QUIC |
| HTTP | HTTP |
| HTTPS | ● HTTP<br>● HTTPS |

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. Haga clic en **Create Backend Server Group** en la esquina superior derecha.
6. Configure la política de enrutamiento basada en **Tabla 4-12**.

**Tabla 4-12** Parámetros necesarios para configurar una política de enrutamiento

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancer Type | Especifica el tipo de balanceadores de carga que pueden utilizar el grupo de servidores backend. Se recomiendan balanceadores de carga dedicados.<br>Los siguientes parámetros se aplican a los balanceadores de carga exclusivos. | - |
| Load Balancer | Especifica si se debe asociar un balanceador de carga.<br>Puede asociar un balanceador de carga dedicado existente al crear un grupo de servidores backend o asociar uno más tarde.<br>● Asociar más tarde<br>● Asociado existente | Associate later |
| Forwarding Mode | Especifica el modo de reenvío para distribuir el tráfico. Hay dos opciones: **Load balancing** y **Active/Standby**.<br>● **Load balancing**: Puede agregar uno o más servidores backend al grupo de servidores backend.<br>● **Active/Standby**: Puede agregar solo dos servidores backend al grupo de servidores backend, uno actuando como servidor activo y el otro como servidor en espera. Si el servidor activo está defectuoso, el tráfico se reenvía al servidor en espera, lo que mejora la confiabilidad del servicio. | Load balancing |
| Backend Server Group Type | Especifica el tipo del grupo de servidores backend.<br>● **Hybrid**: Puede agregar ECS e interfaces de red suplementarias como servidores backend, o agregar direcciones IP como servidores cuando **IP as a Backend** está habilitado.<br>Cuando crea un grupo de servidores backend híbrido, debe especificar una VPC y asociar el grupo de servidores backend con un balanceador de carga en esta VPC.<br>● **IP as a backend server**: Puede agregar direcciones IP como servidores backend solo cuando habilita **IP as a Backend**. | Hybrid |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| VPC | Especifica la VPC donde funciona el grupo de servidores backend. Puede asociar el grupo de servidores backend con un balanceador de carga en esta VPC.<br>Este parámetro es obligatorio si selecciona **Hybrid** para **Backend Server Group Type**.<br>Puede seleccionar una VPC existente o crear una nueva.<br>Para obtener más información acerca de VPC, consulte la ***Guía del usuario de Virtual Private Cloud***. | vpc-test |
| Backend Protocol | Especifica el protocolo que utilizan los servidores backend del grupo de servidores backend para recibir solicitudes de los oyentes. El protocolo varía dependiendo del modo de reenvío:<br>● **Load balancing**: HTTP, HTTPS, TCP, UDP y QUIC<br>● **Active/Standby**: TCP, UDP y QUIC | HTTP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo utilizado por el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: Las solicitudes se enrutan a diferentes servidores en función de sus pesos. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones, a cada servidor se le asigna un peso basado en su capacidad. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: Permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que las solicitudes del mismo cliente se reenvíen al mismo servidor.<br>● **Connection ID**: Este algoritmo está disponible cuando se ha seleccionado **QUIC** para **Backend Protocol**. Este algoritmo permite que las solicitudes con diferentes ID de conexión se enruten a diferentes servidores backend y garantiza que las solicitudes con el mismo ID de conexión se enruten al mismo servidor backend.<br>Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Algoritmos de balanceo de carga**. | Weighted round robin |
| Sticky Session | Especifica si se deben habilitar las sesiones adhesivas si se ha seleccionado **Weighted round robin** o **Weighted least connections** para **Load Balancing Algorithm**.<br>Si habilita las sesiones adhesivas, todas las solicitudes del mismo cliente durante una sesión se envían al mismo servidor backend.<br>Para obtener más información sobre las sesiones adhesivas, consulte **Sesión adhesiva**. | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session Type | Especifica el tipo de sesión adhesiva.<br>Este parámetro es obligatorio si **Sticky Session** está habilitado. Puede seleccionar uno de los siguientes tipos:<br>● **Source IP address**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave de hash única, y todos los servidores backend están numerados. El sistema asigna el cliente a un servidor determinado basándose en la clave generada. Esto permite que las solicitudes de la misma dirección IP se reenvíen al mismo servidor backend.<br>● **Load balancer cookie**: El balanceador de carga genera una cookie después de recibir una solicitud del cliente. Todas las solicitudes posteriores con la cookie se enrutan al mismo servidor backend.<br>**NOTA**<br>● **Source IP address** está disponible cuando se ha seleccionado **TCP**, **QUIC,** o **UDP** para **Backend Protocol**.<br>● **Load balancer cookie** están disponibles cuando seleccionas **HTTP** y **HTTPS** para **Backend Protocol**. | Source IP address |
| Stickiness Duration (min) | Especifica los minutos que se mantienen las sesiones adhesivas. Este parámetro es obligatorio si **Sticky Session** está habilitado.<br>● Sesiones adhesivas en Capa 4: de **1** a **60**<br>● Sesiones adhesivas en Capa 7: de **1** a **1440** | 20 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Slow Start | Especifica si se habilitará el inicio lento. Este parámetro es opcional si ha seleccionado **Weighted round robin** para **Load Balancing Algorithm**.<br>Después de activar esta opción, el balanceador de carga aumenta linealmente la proporción de solicitudes a los servidores backend en este modo.<br>Cuando transcurre la duración de inicio lento, el balanceador de carga envía una parte completa de las solicitudes a los servidores backend y sale del modo de inicio lento.<br>**NOTA**<br>El inicio lento solo está disponible para los grupos de servidores HTTP y HTTPS backend de balanceadores de carga dedicados.<br>Para obtener más información sobre el inicio lento, consulte **Inicio lento (balanceadores de carga dedicados)**. | - |
| Slow Start Duration (s) | Especifica cuánto tiempo durará el inicio lento, en segundos.<br>Este parámetro es obligatorio si **Slow Start** está habilitado. | 30 |
| Description | Proporciona información adicional sobre el grupo de servidores backend. | - |

7. Haga clic en **Next** para agregar servidores backend y configurar la comprobación de estado.

   Agregue servidores en la nube, interfaces de red suplementarias o direcciones IP a este grupo de servidores backend. Para obtener más información, véase **Descripción general**.

   Configure la comprobación de estado para el grupo de servidores backend basado en **Tabla 4-13**. Para obtener más información acerca de los exámenes de salud, consulte **Comprobación de estado**.

   **Tabla 4-13** Parámetros necesarios para configurar una comprobación de estado

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada, haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check Protocol | Especifica el protocolo que utilizará el balanceador de carga para comprobar el estado de los servidores backend.<br>● El protocolo de backend puede ser TCP, HTTP o HTTPS.<br>● Si el protocolo del grupo de servidores backend es UDP, el protocolo de comprobación de estado es UDP de forma predeterminada. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado.<br>Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto se encuentra dentro del rango de 1 a 65535.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS.<br>La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra inclinada (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras (/), puntos (.), signos de interrogación (?), signos numéricos (#), signos de porcentaje (%), ampersands (&) y conjuntos de caracteres extendidos _;~!.() *[]@ $^:',+ | /index.html |
| Interval (s) | Especifica el tiempo máximo entre dos comprobaciones de estado consecutivas, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Especifica el tiempo máximo necesario para esperar una respuesta de la comprobación de estado, en segundos. El intervalo oscila entre **1** y **50**. | 3 |
| Maximum Retries | Especifica el número máximo de reintentos de comprobación de estado. El valor oscila entre **1** y **10**. | 3 |

8. Haga clic en **Next**.
9. Confirme las especificaciones y haga clic en **Create Now**.

## Operaciones relacionadas

Puede asociar el grupo de servidores backend con el oyente de un balanceador de carga dedicado de cualquiera de las formas enumeradas en **Tabla 4-10**.

# 4.4 Creación de un grupo de servidores backend (balanceadores de carga compartidos)

## Escenario

Para enrutar solicitudes, es necesario asociar un grupo de servidores backend a cada oyente.

NOTA

En esta sección se describe cómo crear un grupo de servidores backend para un balanceador de carga compartido.

Puede crear un grupo de servidores backend de las formas que se enumeran en **Tabla 4-14**.

**Tabla 4-14** Creación de un grupo de servidores backend

| Escenario | Procedimiento |
| --- | --- |
| Creación de un grupo de servidores backend y asociarlo con un balanceador de carga | **Procedimiento** |
| Creación de un grupo de servidores backend al agregar un oyente | Puede agregar oyentes utilizando diferentes protocolos según sea necesario. Para obtener más información, véase **Descripción general**.<br>Las referencias son las siguientes:<br>● **Adición de un oyente de TCP**<br>● **Adición de un oyente de UDP**<br>● **Adición de un oyente de HTTP**<br>● **Adición de un oyente de HTTPS** |
| Cambio del grupo de servidores backend asociado al oyente | **Cambio de un grupo de servidores backend** |

## Restricciones

- El protocolo backend del nuevo grupo de servidores backend debe coincidir con el protocolo frontend del oyente como se describe en **Tabla 4-3**.
- El grupo de servidores backend de un balanceador de carga compartido puede asociarse con un solo oyente.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. Haga clic en **Create Backend Server Group** en la esquina superior derecha.
6. Configure la política de enrutamiento basada en **Tabla 4-15**.

**Tabla 4-15** Parámetros necesarios para configurar una política de enrutamiento

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancer Type | Especifica el tipo de balanceadores de carga que pueden utilizar el grupo de servidores backend. | Shared |
| Load Balancer | Especifica si se debe asociar un balanceador de carga. | N/A |
| Backend Server Group Name | Especifica el nombre del grupo de servidores backend. | server_group |
| Backend Protocol | Especifica el protocolo que utilizan los servidores backend del grupo de servidores backend para recibir solicitudes de los oyentes. El protocolo varía dependiendo del modo de reenvío:<br>Las opciones son HTTP, TCP y UDP. | HTTP |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Load Balancing Algorithm | Especifica el algoritmo utilizado por el balanceador de carga para distribuir el tráfico. Las siguientes opciones están disponibles:<br>● **Weighted round robin**: Las solicitudes se enrutan a diferentes servidores en función de sus pesos. Los servidores backend con mayores pesos reciben proporcionalmente más solicitudes, mientras que los servidores con la misma ponderación reciben el mismo número de solicitudes.<br>● **Weighted least connections**: Además del número de conexiones, a cada servidor se le asigna un peso basado en su capacidad. Las solicitudes se enrutan al servidor con la relación de conexiones a ponderación más baja.<br>● **Source IP hash**: Permite que las solicitudes de diferentes clientes se enruten en función de las direcciones IP de origen y garantiza que las solicitudes del mismo cliente se reenvíen al mismo servidor.<br>● **Connection ID**: Este algoritmo está disponible cuando se ha seleccionado **QUIC** para **Backend Protocol**. Este algoritmo permite que las solicitudes con diferentes ID de conexión se enruten a diferentes servidores backend y garantiza que las solicitudes con el mismo ID de conexión se enruten al mismo servidor backend.<br>Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Algoritmos de balanceo de carga**. | Weighted round robin |
| Sticky Sessions | Especifica si se habilitarán las sesiones adhesivas. Si habilita las sesiones adhesivas, todas las solicitudes del mismo cliente durante una sesión se envían al mismo servidor backend.<br>Para obtener más información sobre las sesiones adhesivas, consulte **Sesión adhesiva**. | N/A |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Sticky Session Type | Especifica el tipo de sesiones adhesivas. Después de habilitar la sesión adhesiva, debe seleccionar un tipo de sesión adhesiva:<br>● **Source IP address**: La dirección IP de origen de cada solicitud se calcula utilizando el algoritmo de hash consistente para obtener una clave de hash única, y todos los servidores backend están numerados. El sistema asigna el cliente a un servidor determinado basándose en la clave generada. Esto permite que las solicitudes de diferentes clientes se enruten y garantiza que un cliente se dirija al mismo servidor que estaba usando anteriormente.<br>● **Load balancer cookie**: El balanceador de carga genera una cookie después de recibir una solicitud del cliente. Todas las solicitudes posteriores con la cookie se enrutan al mismo servidor backend.<br>● **Application cookie**: La aplicación desplegada en el servidor backend genera una cookie después de recibir la primera solicitud del cliente. Todas las solicitudes posteriores con la misma cookie se enrutan al mismo servidor backend.<br>**NOTA**<br>● **Source IP address** está disponible cuando se ha seleccionado **TCP**, **UDP** o **QUIC** para **Backend Protocol**.<br>● **Load balancer cookie** está disponible cuando se ha seleccionado **HTTP** o **HTTPS** para **Backend Protocol**. | Source IP address |
| Stickiness Duration (min) | Especifica el tiempo que se mantienen las sesiones adhesivas, en minutos.<br>● Sesiones adhesivas en Capa 4: de **1** a **60**<br>● Sesiones adhesivas en Capa 7: de **1** a **1440** | 20 |
| Description | Proporciona información adicional sobre el grupo de servidores backend. | N/A |

7. Haga clic en **Next** para agregar servidores de back-end y configurar la comprobación de estado basada en **Tabla 4-16**. Para obtener más información acerca de los exámenes de salud, consulte **Comprobación de estado**.

**Tabla 4-16** Parámetros necesarios para configurar una comprobación de estado

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Health Check | Especifica si se habilitarán las comprobaciones de estado.<br>Si la comprobación de estado está habilitada, haga clic en  junto a **Advanced Settings** para establecer los parámetros de comprobación de estado. | N/A |
| Health Check Protocol | ● El protocolo de comprobación de estado puede ser TCP o HTTP.<br>● Si el protocolo del grupo de servidores backend es UDP, el protocolo de comprobación de estado es UDP de forma predeterminada. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. De forma predeterminada, se utiliza la dirección IP privada de cada servidor backend.<br>Un nombre de dominio consta de al menos dos cadenas de caracteres separadas por puntos (.). La longitud total de un nombre de dominio no puede exceder los 100 caracteres con cada cadena de caracteres no superior a 63 caracteres. Solo se permiten letras, dígitos y guiones (-). Las cadenas no pueden comenzar ni terminar con un guion. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto oscila entre **1** y **65535**.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra diagonal (/).<br>La ruta puede contener letras, dígitos, guiones (-), barras (/), puntos (.), signos de interrogación (?), signos numéricos (#), signos porcentuales (%), ampersands (&). | /index.html |
| Interval (s) | Especifica el tiempo máximo entre dos comprobaciones de estado consecutivas, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Especifica el tiempo máximo necesario para esperar una respuesta de la comprobación de estado, en segundos. El intervalo oscila entre **1** y **50**. | 3 |
| Maximum Retries | Especifica el número máximo de reintentos de comprobación de estado. El valor oscila entre **1** y **10**. | 3 |

8. Haga clic en **Next**.
9. Confirme las especificaciones y haga clic en **Create Now**.

# 4.5 Modificación de un grupo de servidores backend

## 4.5.1 Descripción general

Después de crear un grupo de servidores backend, puede modificar su configuración de comprobación de estado e información básica.

### Comprobación de estado

Si los servidores backend tienen que manejar un gran número de solicitudes, las comprobaciones de estado frecuentes pueden sobrecargar los servidores backend y hacer que respondan lentamente. Para solucionar este problema, puede prolongar el intervalo de comprobación de estado o utilizar TCP o UDP en lugar de HTTP. También puede desactivar la comprobación de estado. Si decide desactivar la comprobación de estado, es posible que las solicitudes se enruten a servidores que no estén sanos y que se produzcan interrupciones del servicio.

Para obtener más información sobre el chequeo de salud, consulte **Comprobación de estado**.

Para obtener más información sobre cómo modificar la configuración de la comprobación de estado, consulte **Modificación de la configuración de comprobación de estado**.

### información básica

Puede modificar la información básica de un grupo de servidores backend que aparece en **Tabla 4-17**.

**Tabla 4-17** Información básica que se puede modificar

| Parámetro | Descripción |
| --- | --- |
| Name | Para cambiar el nombre, realice las operaciones de **Cambio del algoritmo de balanceo de carga**. |
| Load Balancing Algorithm | Cambie el algoritmo de balanceo de carga realizando las operaciones de **Cambio del algoritmo de balanceo de carga**.<br>Para obtener más información sobre los algoritmos de balanceo de carga, consulte **Algoritmos de balanceo de carga**. |
| Sticky Session | Habilite o deshabilite la sesión adhesiva realizando las operaciones de **Modificación de la configuración de sesión adhesiva**.<br>Para obtener más información sobre la función de sesión adhesiva, consulte **Sesión adhesiva**. |
| Slow Start | Habilite o deshabilite el inicio lento realizando las operaciones de **Modificación de la configuración de inicio lento (balanceadores de carga dedicados)**.<br>Para obtener más información sobre la función de inicio lento, consulte **Inicio lento (balanceadores de carga dedicados)**. |
| Description | Para cambiar la descripción del grupo de servidores backend, realice las operaciones de **Cambio del algoritmo de balanceo de carga**. |

## 4.5.2 Modificación de la configuración de comprobación de estado

### Escenario

En esta sección se describe cómo puede modificar la configuración de la comprobación de estado.

Después de cambiar el protocolo, el balanceador de carga utiliza el nuevo protocolo para comprobar el estado de los servidores backend. El balanceador de carga continúa enrutando el tráfico a los servidores backend después de que se detectan sanos.

Antes de que las nuevas configuraciones surtan efecto, el balanceador de carga puede devolver el código de error HTTP 503 a los clientes.

NOTA

Esta sección se aplica a los balanceadores de carga dedicados y compartidos.

## Restricciones y notas

- El protocolo de comprobación de estado puede ser diferente del protocolo backend.
- Para reducir el uso de vCPU de los servidores backend, se recomienda que utilice TCP para las comprobaciones de estado. Si desea usar HTTP para las comprobaciones de estado, puede usar archivos estáticos para devolver los resultados de la comprobación de estado.
- Si la comprobación de estado está habilitada, las reglas del grupo de seguridad deben permitir el tráfico desde el puerto de comprobación de estado a los servidores backend a través del protocolo de comprobación de estado.
  - Balanceadores de carga dedicados: Para obtener más información, consulte **Reglas de grupos de seguridad**.
  - Balanceadores de carga compartidos: Para obtener más información, consulte **Reglas de grupos de seguridad**.

NOTA

Después de habilitar la comprobación de estado, el balanceador de carga comprueba inmediatamente el estado de los servidores backend.

- Si se detecta un servidor backend en buen estado, el balanceador de carga iniciará las solicitudes de enrutamiento a él a través de nuevas conexiones basándose en los algoritmos y pesos de balanceo de carga configurados.
- Si se detecta un servidor backend que no está en buen estado, el balanceador de carga dejará de enrutar el tráfico hacia él.

## Habilitar la comprobación de estado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página de ficha **Backend Server Groups**, busque el grupo de servidores backend.
6. En la página **Summary**, haga clic en **Health Check** a la derecha.
7. En el cuadro de diálogo **Configure Health Check**, configure los parámetros basados en **Tabla 4-18**.

**Tabla 4-18** Parámetros necesarios para configurar la comprobación de estado

| Parámetro | Descripción | Valor de ejemplo |
|---|---|---|
| Comprobación de estado | Especifica si se habilitarán las comprobaciones de estado. | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Protocolo de comprobación de estado | ● El protocolo de comprobación de estado puede ser TCP, HTTP o HTTPS.<br>● Si el protocolo del grupo de servidores backend es UDP, el protocolo de comprobación de estado es UDP de forma predeterminada. | HTTP |
| Domain Name | Especifica el nombre de dominio que se utilizará para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS.<br>● Puede utilizar la dirección IP privada del servidor backend como nombre de dominio.<br>● También puede especificar un nombre de dominio que consta de al menos dos etiquetas separadas por puntos (.). Use solo letras, dígitos y guiones (-). No inicie o termine cadenas con un guion. Máximo total: 100 caracteres. Etiqueta máxima: 63 caracteres. | www.elb.com |
| Health Check Port | Especifica el puerto que utilizará el balanceador de carga para comprobar el estado de los servidores backend. El número de puerto oscila entre **1** y **65535**.<br>**NOTA**<br>De forma predeterminada, se utiliza el puerto de servicio en cada servidor backend. También puede especificar un puerto para las comprobaciones de estado. | 80 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Path | Especifica la dirección URL de comprobación de estado, que es el destino de los servidores backend para las comprobaciones de estado. Este parámetro es obligatorio si el protocolo de comprobación de estado es HTTP o HTTPS. La ruta puede contener de 1 a 80 caracteres y debe comenzar con una barra diagonal (/).<br>● Si el grupo de servidores backend está asociado con un balanceador de carga dedicado, la ruta de comprobación puede contener letras, dígitos, guiones (-), barras (/), puntos (.), signos de interrogación (?), signos numéricos (#), signos de porcentaje (%), ampersands (&) y conjuntos de caracteres extendidos_;~!.() *[]@ $^:',+<br>● Si el grupo de servidores back-end está asociado a un balanceador de carga compartido, la ruta puede contener letras, dígitos, guiones (-), barras (/), puntos (.), signos de interrogación (?), signos de porcentaje (%), ampersands (&) y caracteres extendidos _ | /index.html |
| Interval (s) | Especifica el tiempo máximo entre dos comprobaciones de estado consecutivas, en segundos.<br>El intervalo oscila entre **1** y **50**. | 5 |
| Timeout (s) | Especifica el tiempo máximo necesario para esperar una respuesta de la comprobación de estado, en segundos. El intervalo oscila entre **1** y **50**. | 3 |
| Maximum Retries | Especifica el número máximo de reintentos de comprobación de estado. El valor oscila entre **1** y **10**. | 3 |

8. Haga clic en **OK**.

## Deshabilitar la comprobación de estado

1. Inicie sesión en la consola de gestión.

2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend de destino.
6. En la página **Summary**, haga clic en **Health Check** a la derecha.
7. En el cuadro de diálogo **Configure Health Check**, deshabilite la comprobación de estado.
8. Haga clic en **OK**.

## 4.5.3 Cambio del algoritmo de balanceo de carga

### Escenario

Esta sección describe cómo puede cambiar el algoritmo de balanceo de carga.

Para obtener más información sobre los algoritmos de balanceo de carga, consulte **Algoritmos de balanceo de carga**.

NOTA

Esta sección se aplica a los balanceadores de carga dedicados y compartidos.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, busque el grupo de servidores backend de destino y haga clic en **Edit** en la columna **Operation**.
6. En el cuadro de diálogo **Modify Backend Server Group**, cambie el algoritmo de balanceo de carga.
7. Haga clic en **OK**.

NOTA

El nuevo algoritmo de balanceo de carga entra en vigor inmediatamente y se utilizará para enrutar solicitudes a través de nuevas conexiones. Sin embargo, el algoritmo de equilibrio de carga anterior todavía se utilizará para enrutar solicitudes a través de conexiones establecidas.

# 4.5.4 Modificación de la configuración de sesión adhesiva

## Escenario

En esta sección se describe cómo puede modificar la configuración de la sesión adhesiva.

NOTA

- Esta sección se aplica a los balanceadores de carga dedicados y compartidos.
- También puede configurar sesiones adhesivas al agregar un oyente o crear un grupo de servidores backend.

## Habilitación de sesión adhesiva

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, busque el grupo de servidores backend y haga clic en **Edit** en la columna **Operation**.
6. En el cuadro de diálogo **Modify Backend Server Group**, habilite la sesión adhesiva, seleccione el tipo de sesión adhesiva y establezca la duración de la sesión.
7. Haga clic en **OK**.

## Desactivación de sesión adhesiva

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, busque el grupo de servidores backend y haga clic en **Edit** en la columna **Operation**.
6. En el cuadro de diálogo **Modify Backend Server Group**, deshabilite la sesión adhesiva.
7. Haga clic en **OK**.

# 4.5.5 Modificación de la configuración de inicio lento (balanceadores de carga dedicados)

## Escenario

Esta sección describe cómo puede modificar la configuración de inicio lento.

Para obtener más información, véase **Inicio lento (balanceadores de carga dedicados)**.

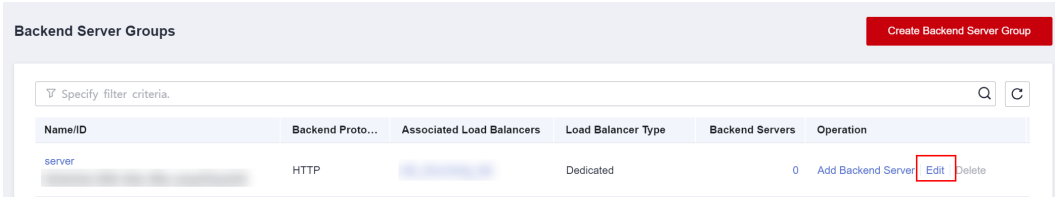
NOTA

- Esta sección solo se aplica a los balanceadores de carga dedicados.
- También puede configurar el inicio lento al agregar un oyente o crear un grupo de servidores backend.

## Habilitación de inicio lento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, busque el grupo de servidores backend y haga clic en **Edit** en la columna **Operation**.

   **Figura 4-11** Modificación de un grupo de servidores backend

6. En el cuadro de diálogo **Modify Backend Server Group**, habilite el inicio lento y establezca la duración del inicio lento.

   La duración de inicio lento oscila entre 30 y 1200 en segundos. Cuando transcurre la duración de inicio lento, el balanceador de carga envía una parte completa de las solicitudes a los servidores backend y sale del modo de inicio lento.
7. Haga clic en **OK**.

## Desactivación del inicio lento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, busque el grupo de servidores backend y haga clic en **Edit** en la columna **Operation**.
6. En el cuadro de diálogo **Modify Backend Server Group**, deshabilite el inicio lento.
7. Haga clic en **OK**.

# 4.6 Cambio de un grupo de servidores backend

## Escenario

Esta sección describe cómo puede cambiar el grupo de servidores backend predeterminado configurado para un oyente.

Los oyentes TCP o UDP reenvían las solicitudes a los grupos de servidores de backend predeterminados.

Los oyentes HTTP o HTTPS reenvían solicitudes basadas en las prioridades de las políticas de reenvío. Si no agrega una política de reenvío, el oyente enrutará las solicitudes al grupo de servidores backend predeterminado.

## Restricciones y limitaciones

- El grupo de servidores backend no se puede cambiar si la redirección está habilitada.
- El protocolo backend del grupo de servidores backend debe coincidir con el protocolo frontend del oyente. Para obtener más información, véase **Tabla 4-3**.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga de destino y haga clic en su nombre.
5. En la ficha **Listeners**, localice el oyente de destino y haga clic en su nombre.
6. En la página **Summary**, haga clic en **Change Backend Server Group** a la derecha.
7. En el cuadro de diálogo que se muestra, haga clic en el cuadro de nombre del grupo de servidores.

   Seleccione un grupo de servidores backend de la lista desplegable o cree un grupo.

   a. Haga clic en el nombre del grupo de servidores backend o escriba el nombre en el cuadro de búsqueda para buscar el grupo de destino.

b. Haga clic en **Create Backend Server Group**. Después de crear el grupo de servidores backend, haga clic en el icono de actualización.

NOTA

El protocolo backend del nuevo grupo de servidores backend debe coincidir con el protocolo frontend del oyente.

8. Haga clic en **OK**.

# 4.7 Consulta de un grupo de servidores backend

## Escenario

En esta sección se describe cómo puede ver la siguiente información sobre un grupo de servidores backend:

- Información básica: el nombre, el ID y el protocolo de backend
- Comprobación de estado: si la comprobación de estado está habilitada y las configuraciones de comprobación de estado
- Servidores backend: servidores que se han agregado al grupo de servidores backend

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. En la página de ficha **Summary**, vea la información básica y la configuración de comprobación de estado.

# 4.8 Eliminación de un grupo de servidores backend

## Escenario

En esta sección se describe cómo eliminar un grupo de servidores backend.

## Restricciones y limitaciones

- Antes de eliminar un grupo de servidores backend, debe:
  - Desvincularlo del oyente. Para obtener más información, véase **Cambio de un grupo de servidores backend**.
  - Asegúrese de que el grupo de servidores backend no es utilizado por una política de reenvío de un oyente HTTP o HTTPS.

- Quite todos los servidores backend del grupo de servidores backend.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, busque el grupo de servidores backend y haga clic en **Delete** en la columna **Operation**.
6. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

# 5 Servidor backend (balanceador de carga dedicado)

## 5.1 Descripción general

Los servidores backend reciben y procesan solicitudes del balanceador de carga asociado.

Si el tráfico entrante aumenta, puede agregar más servidores backend para garantizar la estabilidad y confiabilidad de las aplicaciones y eliminar los puntos únicos de falla. Si el tráfico entrante disminuye, puede quitar algunos servidores backend para reducir el costo.

Si el balanceador de carga está asociado a un grupo de AS, las instancias se agregan o quitan automáticamente del balanceador de carga.

Se pueden agregar diferentes tipos de servidores backend a diferentes tipos de grupos de servidores backend como se describe en **Tabla 5-1**.

**Tabla 5-1** Grupo de servidores backend y tipos de servidores backend

| Tipo de grupo de servidores backend | Tipos de servidor backend | Referencia |
| --- | --- | --- |
| Híbrido | • Servidores en la nube o interfaces de red suplementarias que estén en la misma VPC que el balanceador de carga, si **IP as a Backend** está deshabilitado<br>• Direcciones IP de servidores en otras VPC o en su centro de datos local, si **IP as a Backend** está habilitado<br>**NOTA**<br>Cuando crea un grupo de servidores backend híbrido, debe especificar una VPC y asociar el grupo de servidores backend con un balanceador de carga en esta VPC. | • **Adición de servidores backend**<br>• **Adición de interfaces de red suplementarias**<br>• **Adición de direcciones IP como servidores backend** |

| Tipo de grupo de servidores backend | Tipos de servidor backend | Referencia |
| --- | --- | --- |
| IP como servidor backend | Direcciones IP de servidores en la nube o locales<br>**NOTA**<br>**IP as a Backend** debe haber sido habilitado para el balanceador de carga. | ● **Adición de direcciones IP como servidores backend** |

## Precauciones

- Se recomienda que seleccione servidores backend que ejecuten el mismo sistema operativo para facilitar la gestión y el mantenimiento.
- El balanceador de carga comprueba el estado de cada servidor agregado al grupo de servidores backend asociado si ha configurado la comprobación del estado para el grupo de servidores backend. Si el servidor backend responde normalmente, el balanceador de carga lo considerará saludable. Si el servidor backend no responde normalmente, el balanceador de carga comprobará periódicamente su estado hasta que el servidor backend se considere saludable.
- Si se detiene o reinicia un servidor backend, las conexiones establecidas con el servidor se desconectarán y los datos que se transmitan a través de estas conexiones se perderán. Para evitar que esto ocurra, configure la función de reintento en los clientes para evitar la pérdida de datos.
- Si habilita las sesiones adhesivas, el tráfico a los servidores backend puede estar desequilibrado. Si esto sucede, deshabilite las sesiones adhesivas y compruebe las solicitudes recibidas por cada servidor backend.

## Restricciones y limitaciones

- Se puede agregar un máximo de 500 servidores backend a un grupo de servidores backend.
- Las reglas de grupo de seguridad entrante deben configurarse para permitir el tráfico a través del puerto de cada servidor backend y puerto de comprobación de estado. Para obtener más información, véase **Reglas de grupos de seguridad**.
- Si selecciona solo el equilibrio de carga de red, un servidor no puede servir como servidor backend y como cliente.

## Ponderación del servidor backend

Necesita establecer una ponderación para cada servidor backend en un grupo de servidores backend para recibir solicitudes. Cuanto mayor sea el peso que haya configurado para un servidor backend, más solicitudes recibirá el servidor backend.

Puede establecer un entero de **0** a **100**. Si establece la ponderación de un servidor backend en **0**, las nuevas solicitudes no se encaminarán a este servidor.

Tres algoritmos de balanceo de carga le permiten establecer ponderaciones para servidores backend, como se muestra en la siguiente tabla. Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Algoritmos de balanceo de carga**.

**Tabla 5-2** Ponderaciones del servidor en diferentes algoritmos de balanceo de carga

| Algoritmo de balanceo de carga | Ajuste de ponderación |
| --- | --- |
| Round robin ponderado | ● Si ninguno de los servidores backend tiene una ponderación de 0, el balanceador de carga enruta las solicitudes a los servidores backend en función de sus ponderaciones. Los servidores backend con ponderaciones más altas reciben proporcionalmente más solicitudes.<br>● Si dos servidores backend tienen la misma ponderación, reciben el mismo número de solicitudes. |
| Planificación por menor número de conexiones y ponderación (weighted least connections) | ● Si ninguno de los servidores backend tiene una ponderación de 0, el balanceador de carga calcula la carga de cada servidor backend usando la fórmula (Overhead = Número de conexiones actuales/ponderación del servidor backend).<br>● El balanceador de carga enruta las solicitudes al servidor backend con la sobrecarga más baja. |
| Hash de IP de origen | ● Si ninguno de los servidores backend tiene una ponderación de 0, las solicitudes del mismo cliente se enrutan al mismo servidor backend dentro de un período de tiempo.<br>● Si la ponderación de un servidor backend es 0, no se enrutan solicitudes a este servidor backend. |

# 5.2 Reglas de grupos de seguridad

## Escenarios

Para garantizar las comunicaciones normales entre el balanceador de carga y los servidores backend, debe comprobar las reglas de grupo de seguridad y las reglas de ACL de red configuradas para los servidores backend.

- Las reglas de grupo de seguridad deben permitir el tráfico desde la subred backend donde reside el balanceador de carga hacia los servidores backend. (De forma predeterminada, la subred de fondo de un balanceador de carga es la misma que la subred donde reside el balanceador de carga.) Para obtener más información acerca de cómo configurar reglas de grupo de seguridad, consulte **Configuración de reglas de grupo de seguridad**.
- Las reglas de ACL de red son opcionales para las subredes. Si se configuran reglas de ACL de red para la subred backend del balanceador de carga, las reglas de ACL de red deben permitir el tráfico desde la subred backend del balanceador de carga a los servidores backend. Para obtener más información acerca de cómo configurar las reglas de ACL de red, consulte **Configuración de reglas de ACL de red**.

NOTA

Si el balanceador de carga tiene un oyente de TCP o de UDP y la IP como backend está deshabilitado, las reglas de grupo de seguridad y las reglas de ACL de red no tendrán efecto.

Puede usar el control de acceso para limitar qué direcciones IP pueden acceder al oyente. Más información sobre cómo configurar **Control de acceso**.

## Restricciones y limitaciones

- Si la comprobación de estado está habilitada para un grupo de servidores backend, las reglas del grupo de seguridad deben permitir el tráfico desde el puerto de comprobación de estado a través del protocolo de comprobación de estado.
- Si UDP se utiliza para la comprobación de estado, debe haber una regla que permita que el tráfico ICMP compruebe el estado de los servidores backend.

## Configuración de reglas de grupo de seguridad

Si no tiene las VPC al crear un servidor, el sistema crea automáticamente una para usted. Las reglas de grupo de seguridad predeterminadas solo permiten comunicaciones entre los servidores de la VPC. Para asegurarse de que el balanceador de carga puede comunicarse con estos servidores tanto a través del puerto frontend como del puerto de comprobación de estado, configure las reglas entrantes para los grupos de seguridad que contienen estos servidores.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. En **Compute**, haga clic en **Elastic Cloud Server**.
4. En la página **Elastic Cloud Server**, haga clic en el nombre del ECS que se ha agregado a un grupo de servidores backend.

   Se mostrará la página que proporciona los detalles del ECS.
5. Haga clic en **Security Groups**, busque el grupo de seguridad y vea las reglas del grupo de seguridad.
6. Haga clic en el ID de una regla o **Modify Security Group Rule** de grupo de seguridad. Se muestra la página de detalles del grupo de seguridad.
7. En la página de ficha **Inbound Rules**, haga clic en **Add Rule**. Configure una regla de entrada basada en **Tabla 5-3**.

**Tabla 5-3** Reglas de grupos de seguridad

| Protocolo backend | Política | Protocolo & Puerto | Dirección IP de origen |
|---|---|---|---|
| HTTP o HTTPS | Permitir | **Protocol**: TCP<br>**Port**: el puerto utilizado por el servidor back-end y el puerto de comprobación de estado | Subred backend del balanceador de carga |
| TCP | Permitir | **Protocol**: TCP<br>**Port**: puerto de comprobación de estado | |

| Protocolo backend | Política | Protocolo & Puerto | Dirección IP de origen |
| --- | --- | --- | --- |
| UDP | Permitir | **Protocol**: UDP e ICMP<br>**Port**: puerto de comprobación de estado | |

NOTA

- Después de crear un balanceador de carga, no cambie la subred. Si se cambia la subred, las direcciones IP ocupadas por el balanceador de carga no se liberarán, y el tráfico de la subred de backend anterior aún debe permitirse a los servidores de backend.
- También es necesario permitir el tráfico de la nueva subred de backend a los servidores de backend.

8. Haga clic en **OK**.

## Configuración de reglas de ACL de red

Para controlar el tráfico dentro y fuera de una subred, puede asociar una ACL de red a la subred. Las reglas de ACL de red controlan el acceso a las subredes y agregan una capa adicional de defensa a las subredes.

La regla de ACL de red predeterminada deniega todo el tráfico entrante y saliente. Puede configurar una regla de entrada para permitir el tráfico desde la subred de backend del balanceador de carga a través del puerto del servidor de backend.

- Si el balanceador de carga está en la misma subred que los servidores backend, las reglas de ACL de red no tendrán efecto. En este caso, los servidores backend se considerarán sanos y podrán ser accedidos por los clientes.
- Si el balanceador de carga no está en la misma subred que los servidores backend, las reglas de ACL de red tendrán efecto. En este caso, los servidores backend se considerarán insalubres y no podrán ser accedidos por los clientes.

NOTA

Las reglas de ACL de red configuradas para la subred de backend del balanceador de carga no restringirán el tráfico de los clientes al balanceador de carga. Si se configuran las reglas de ACL de red, los clientes pueden acceder directamente al balanceador de carga. Para controlar el acceso al balanceador de carga, configure el control de acceso para todos los oyentes agregados al balanceador de carga realizando las operaciones de **Control de acceso**.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el cursor sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Network ACLs**.

5. En la lista de ACL de red, haga clic en el nombre del ACL de red para cambiar a la página que muestra sus detalles.
6. En la ficha **Inbound Rules** o **Outbound Rules**, haga clic en **Add Rule** para agregar una regla de entrada o de salida.
   - **Action**: Seleccione **Allow**.
   - **Type**: Seleccione el mismo tipo que la subred backend del balanceador de carga.
   - **Protocol**: El protocolo debe ser el mismo que el protocolo backend.
   - **Source**: Configúrelo en la subred de backend del balanceador de carga.
   - **Source Port Range**: Seleccione un rango de puertos.
   - **Destination**: Ingrese una dirección de destino permitida en esta dirección. El valor predeterminado es **0.0.0.0/0**, que indica que se permite el tráfico de todas las direcciones IP.
   - **Destination Port Range**: Seleccione un rango de puertos.
   - (Opcional) **Description**: Describa la regla de ACL de red.
7. Haga clic en **OK**.

# 5.3 Gestión de servidores backend

## 5.3.1 Adición de servidores backend

### Escenario

Cuando utiliza ELB para enrutar el tráfico a los servidores backend, debe asegurarse de que al menos un servidor backend se está ejecutando correctamente y puede recibir solicitudes del balanceador de carga asociado.

Si el tráfico entrante aumenta, puede agregar más servidores backend para garantizar la estabilidad y confiabilidad de las aplicaciones y eliminar los puntos únicos de falla. Si el tráfico entrante disminuye, puede quitar algunos servidores backend para reducir el costo.

### Restricciones y limitaciones

- Los servidores en la nube deben estar en la misma VPC que el grupo de servidores backend.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.

6. Cambie a la página de pestaña **Backend Servers** y haga clic en **Add** a la derecha.
7. Puede buscar servidores backend utilizando palabras clave especificadas.

   Seleccione los servidores backend que desea agregar y haga clic en **Next**.
8. Especifique las ponderaciones y puertos para los servidores backend y haga clic en **Finish**.

   Los puertos de servidor backend se pueden establecer por lotes.

# 5.3.2 Consulta de servidores backend

## Escenario

Puede ver los servidores backend que se han agregado a un grupo de servidores backend, incluidos su estado, direcciones IP privadas, resultados de comprobación de estado, ponderaciones y puertos.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Backend Servers**.
7. En la lista de servidores backend, vea los servidores backend.

# 5.3.3 Extracción de servidores backend

## Escenario

Puede quitar un servidor backend que ya no sea necesario de un grupo de servidores backend.

Una vez que se quita un servidor backend, se desvincula del balanceador de carga y ya no recibirá solicitudes del balanceador de carga. El servidor backend aún existe. Puede agregar el servidor backend al grupo de servidores backend de nuevo cuando aumente el tráfico o se necesite mejorar la confiabilidad.

## Notas

Después de quitar el servidor backend, las solicitudes siguen siendo enviadas a él. Esto se debe a que se establece una conexión persistente entre el balanceador de carga y el servidor backend y las solicitudes se enrutan a este servidor hasta que se agote el tiempo de espera de la conexión de TCP.

Si no se transmiten datos a través de esta conexión de TCP después de que se agote el tiempo, ELB desconecta la conexión.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Backend Servers**.
7. Seleccione los servidores backend que desea quitar y haga clic en **Remove** encima de la lista de servidores backend.
8. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

## 5.3.4 Cambio de las ponderaciones/puertos del servidor backend

### Escenario

Puede cambiar las ponderaciones/puertos configurados para servidores backend en función de su capacidad para procesar solicitudes.

### Restricciones y limitaciones

- Puede establecer un entero de **0** a **100**. Si establece la ponderación de un servidor backend en **0**, las nuevas solicitudes no se encaminarán a este servidor.
- Las ponderaciones solo se pueden especificar cuando se selecciona round robin ponderado, conexiones mínimas ponderadas o hash IP de origen como algoritmo de balanceo de carga. Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Ponderación del servidor backend**.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Backend Servers**.
7. Seleccione los servidores backend y haga clic en **Modify Port/Weight** encima de la lista de servidores backend.

8. En el cuadro de diálogo que se muestra, modifique las ponderaciones/puertos según lo necesite.
   - Modificación de puertos:
     - Cambiar el puerto de un único servidor backend: Configure el puerto en la columna **Backend Port**.
     - Cambiar los puertos de varios servidores backend: Configure los puertos junto a **Batch Modify Ports** y haga clic en **OK**.
   - Modificación de ponderaciones:
     - Cambiar la ponderación de un único servidor backend: Establezca la ponderación en la columna **New Weight**.
     - Cambiar las ponderaciones de varios servidores backend: Establezca la ponderación junto a **Batch Modify Weights** y haga clic en **OK**.

     NOTA

     Puede cambiar las ponderaciones de varios servidores backend a **0** para que no reciban solicitudes del balanceador de carga.
9. Haga clic en **OK**.

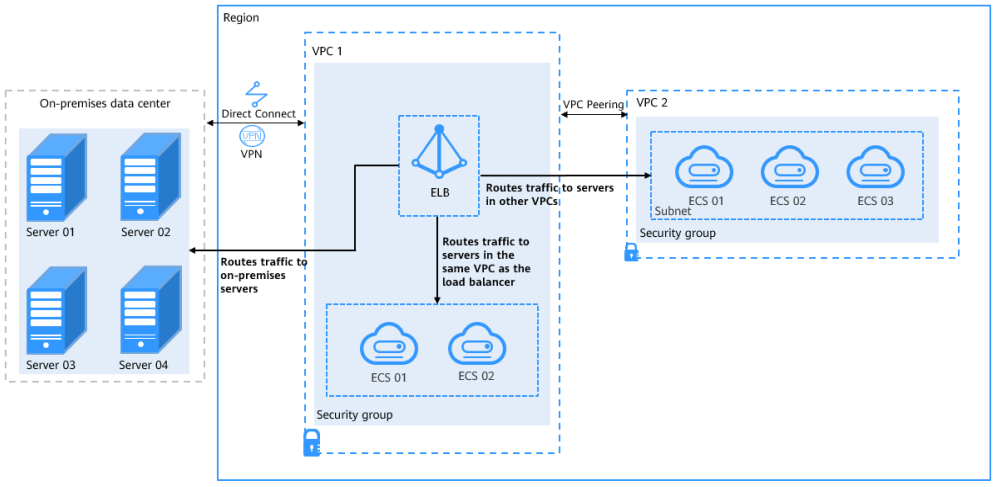
# 5.4 Direcciones IP como servidores backend

## 5.4.1 Descripción general

Los balanceadores de carga dedicados admiten el equilibrio de carga híbrido. Puede agregar servidores e interfaces de red suplementarias en la VPC donde se crea el balanceador de carga, en una VPC diferente o en un centro de datos local, mediante el uso de direcciones IP privadas de los servidores al grupo de servidores backend del balanceador de carga.

De esta manera, el tráfico entrante se puede distribuir de forma flexible a servidores en la nube y servidores locales.

**Figura 5-1** Enrutamiento de solicitudes a servidores en la nube y locales



## Restricciones y limitaciones

- IP as a Backend no se puede deshabilitar después de activar.
- Solo se pueden agregar direcciones IPv4 privadas como servidores backend.
- Se puede establecer un máximo de 50,000 conexiones simultáneas con un servidor backend que se agrega mediante su dirección IP.
- Si agrega direcciones IP como servidores backend, las direcciones IP de origen de los clientes no se pueden pasar a estos servidores. Instale el **módulo TOA** para obtener direcciones IP de origen.

## Escenario

Después de habilitar IP como backend, puede agregar servidores backend usando sus direcciones IP. Es necesario prepararse para diferentes escenarios como se muestra en **Tabla 5-4**.

**Tabla 5-4** Adición de direcciones IP como servidores backend

| Donde se están ejecutando los servidores | Preparaciones |
| --- | --- |
| En una VPC diferente del balanceador de carga | Configure una interconexión de VPC entre la VPC donde se está ejecutando el balanceador de carga y la VPC donde se están ejecutando los servidores.<br>Para obtener más información sobre cómo configurar una interconexión de VPC, consulte la **Guía del usuario de Virtual Private Cloud**. |
| In the same VPC as the load balancer | Configure una interconexión de VPC para la VPC donde se están ejecutando el balanceador de carga y los servidores y, a continuación, agregue rutas para la interconexión de VPC.<br>Para obtener más información, consulte **Enrutamiento de tráfico a servidores backend en la misma VPC que el balanceador de carga**. |
| In on-premises data centers | Conecte el centro de datos local a la VPC donde se ejecuta el balanceador de carga con Direct Connect o VPN. Para obtener más información sobre cómo conectar centros de datos locales a la nube, consulte la **Guía del usuario de Direct Connect** o la **Guía del usuario de Virtual Private Network**. |

# 5.4.2 Habilitación de IP as a Backend

## Escenario

Puede habilitar IP as a Backend para un balanceador de carga dedicado existente.

## Restricciones y limitaciones

- IP as a Backend no se puede deshabilitar después de activar.
- El protocolo de los grupos de servidores backend solo puede ser TCP, UDP, HTTP o HTTPS.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En la página **Load Balancers**, busque el balanceador de carga y haga clic en su nombre.
5. En la página de la ficha **Summary**, haga clic en **Enable** junto a **IP as a Backend**.
6. Haga clic en **OK**.

# 5.4.3 Adición de direcciones IP como servidores backend

## Escenario

Si habilita IP como backend, puede asociar servidores backend con el balanceador de carga mediante sus direcciones IP.

Es necesario prepararse para diferentes escenarios como se muestra en **Tabla 5-5**.

**Tabla 5-5** Adición de direcciones IP como servidores backend

| Donde se están ejecutando los servidores | Preparaciones |
| --- | --- |
| En una VPC diferente del balanceador de carga | Configure una interconexión de VPC entre la VPC donde se está ejecutando el balanceador de carga y la VPC donde se están ejecutando los servidores.<br>Para obtener más información sobre cómo configurar una interconexión de VPC, consulte la **Guía del usuario de Virtual Private Cloud**. |
| In the same VPC as the load balancer | Configure una interconexión de VPC para la VPC donde se están ejecutando el balanceador de carga y los servidores y, a continuación, agregue rutas para la interconexión de VPC.<br>Para obtener más información, consulte **Enrutamiento de tráfico a servidores backend en la misma VPC que el balanceador de carga**. |

| Donde se están ejecutando los servidores | Preparaciones |
| --- | --- |
| In on-premises data centers | Conecte el centro de datos local a la VPC donde se ejecuta el balanceador de carga con Direct Connect o VPN. Para obtener más información sobre cómo conectar centros de datos locales a la nube, consulte la **Guía del usuario de Direct Connect** o la **Guía del usuario de Virtual Private Network**. |

## Restricciones y limitaciones

- Si IP como backend no está habilitado al crear un balanceador de carga, puede habilitarlo en la página **Summary** del balanceador de carga.
- Solo se pueden agregar direcciones IPv4 privadas como servidores backend.
- La subred backend del balanceador de carga debe tener suficientes direcciones IP (al menos 16 direcciones IP). De lo contrario, los servidores backend no se pueden agregar con direcciones IP. Si las direcciones IP son insuficientes, puede agregar más subredes de backend en la página **Summary** del balanceador de carga.
- Las reglas de grupo de seguridad de los servidores backend agregados con direcciones IP deben permitir el tráfico desde la subred backend del balanceador de carga. Si no se permite el tráfico, las comprobaciones de estado fallarán.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de pestaña **Backend Servers** y haga clic en **Add** en el área **IP as Backend Servers**.
7. Especifique las direcciones IP, los puertos y las ponderaciones de los servidores backend.
8. Haga clic en **OK**.

# 5.4.4 Consulta de servidores backend

## Escenario

Puede ver los servidores backend agregados a un grupo de servidores backend, incluidas sus direcciones IP, resultados de comprobación de estado, ponderaciones y puertos.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **IP as Backend Servers**.
7. En la lista de servidores backend, vea los servidores backend agregados.

# 5.4.5 Extracción de servidores backend

## Escenario

Puede quitar servidores backend de un grupo de servidores backend cuando no los necesite para procesar solicitudes.

## Notas

Después de quitar el servidor backend, las solicitudes siguen siendo enviadas a él. Esto se debe a que se establece una conexión persistente entre el balanceador de carga y el servidor backend y las solicitudes se enrutan a este servidor hasta que se agote el tiempo de espera de la conexión de TCP.

Si no se transmiten datos a través de esta conexión de TCP después de que se agote el tiempo, ELB desconecta la conexión.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **IP as Backend Servers**.
7. Seleccione los servidores backend que se van a quitar y haga clic en **Remove** encima de la lista de servidores backend.
8. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

# 5.4.6 Cambio de las ponderaciones/puertos del servidor backend

## Escenario

Puede cambiar las ponderaciones y puertos especificados para los servidores backend en función de su capacidad para procesar solicitudes.

## Restricciones y limitaciones

- Puede establecer un entero de **0** a **100**. Si establece la ponderación de un servidor backend en **0**, las nuevas solicitudes no se encaminarán a este servidor.
- Las ponderaciones solo se pueden especificar cuando se selecciona round robin ponderado, conexiones mínimas ponderadas o hash IP de origen como algoritmo de balanceo de carga. Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Ponderación del servidor backend**.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **IP as Backend Servers**.
7. Seleccione los servidores backend y haga clic en **Modify Port/Weight** en la lista de servidores backend.
8. En el cuadro de diálogo mostrado, modifique las ponderaciones y los puertos según lo necesite.
   - Modificación de puertos:
     - Cambiar el puerto de un único servidor backend: Configure el puerto en la columna **Backend Port**.
     - Cambiar los puertos de varios servidores backend: Configure los puertos junto a **Batch Modify Ports** y haga clic en **OK**.
   - Modificación de ponderaciones:
     - Cambiar la ponderación de un único servidor backend: Establezca la ponderación en la columna **New Weight**.
     - Cambiar las ponderaciones de varios servidores backend: Establezca la ponderación junto a **Batch Modify Weights** y haga clic en **OK**.

     NOTA

     Puede cambiar las ponderaciones de varios servidores backend a **0** para que no reciban solicitudes del balanceador de carga.

9. Haga clic en **OK**.

# 5.5 Interfaces de red suplementarias

## 5.5.1 Adición de interfaces de red suplementarias

### Escenario

Además de los servidores en la nube y los servidores locales, puede agregar interfaces de red suplementarias a un grupo de servidores backend.

Las interfaces de red complementarias le permiten configurar más NICs de las que un servidor en la nube normalmente admitiría. Se pueden conectar a subinterfaces VLAN de interfaces de red elásticas.

Para obtener más información sobre cómo crear una VPC, consulte la *Guía del usuario de Virtual Private Cloud*.

NOTA

Para las regiones en las que se admiten interfaces de red suplementarias, consulte la **Descripción de funciones**.

### Restricciones y limitaciones

Las interfaces de red suplementarias solo se pueden agregar a un grupo de servidores backend híbrido.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend al que desea agregar interfaces de red suplementarias.
6. Cambie a la página de pestaña **Backend Servers** y haga clic en **Add** en el área **Supplementary Network Interfaces**.

   Puede buscar interfaces de red suplementarias por ID, dirección IP privada, dirección IP privada de interfaz de red, nombre de subred o ID de subred.
7. Especifique las ponderaciones y los puertos para las interfaces de red suplementarias y haga clic en **Finish**.

# 5.5.2 Consulta de interfaces de red suplementarias.

## Escenario

Puede ver las interfaces de red suplementarias que se han agregado a un grupo de servidores backend.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Supplementary Network Interfaces**.
7. Vea las interfaces de red suplementarias agregadas.

# 5.5.3 Extracción de interfaces de red suplementarias

## Escenario

Puede quitar interfaces de red suplementarias de un grupo de servidores backend si no las necesita para procesar solicitudes.

## Notas

Después de quitar el servidor backend, las solicitudes siguen siendo enviadas a él. Esto se debe a que se establece una conexión persistente entre el balanceador de carga y el servidor backend y las solicitudes se enrutan a este servidor hasta que se agote el tiempo de espera de la conexión de TCP.

Si no se transmiten datos a través de esta conexión de TCP después de que se agote el tiempo, ELB desconecta la conexión.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.

4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Supplementary Network Interfaces**.
7. Seleccione las interfaces de red suplementarias y haga clic en **Remove** encima de la lista.
8. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

# 5.5.4 Cambio de las ponderaciones/puertos de las interfaces de red suplementarias

## Escenario

Puede cambiar las ponderaciones especificadas para las interfaces de red suplementarias en función de su capacidad para procesar solicitudes.

## Restricciones y limitaciones

- Puede establecer un entero de **0** a **100**. Si establece la ponderación de un servidor backend en **0**, las nuevas solicitudes no se encaminarán a este servidor.
- Las ponderaciones solo se pueden especificar cuando se selecciona round robin ponderado, conexiones mínimas ponderadas o hash IP de origen como algoritmo de balanceo de carga. Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Ponderación del servidor backend**.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Supplementary Network Interfaces**.
7. Seleccione los servidores backend y haga clic en **Modify Weight** en la lista de servidores backend.
8. En el cuadro de diálogo mostrado, modifique las ponderaciones y los puertos según lo necesite.
   - Modificación de puertos:
     - Cambiar el puerto de un único servidor backend: Configure el puerto en la columna **Backend Port**.

- Cambiar los puertos de varios servidores backend: Configure los puertos junto a **Batch Modify Ports** y haga clic en **OK**.

– Modificación de ponderaciones:

- Cambiar la ponderación de un único servidor backend: Establezca la ponderación en la columna **Weight**.
- Cambiar las ponderaciones de varios servidores backend: Establezca la ponderación junto a **Batch Modify Weights** y haga clic en **OK**.

  NOTA

  Puede cambiar las ponderaciones de varios servidores backend a **0** para que no reciban solicitudes del balanceador de carga.

9. Haga clic en **OK**.

# 6 Servidor Backend (balanceadores de carga compartidos)

## 6.1 Descripción general

Los servidores backend reciben y procesan solicitudes del balanceador de carga asociado.

Si el tráfico entrante aumenta, puede agregar más servidores backend para garantizar la estabilidad y confiabilidad de las aplicaciones y eliminar los SPOF. Si el tráfico entrante disminuye, puede quitar algunos servidores backend para reducir el costo.

Si el balanceador de carga está asociado a un grupo de AS, las instancias se agregan o quitan automáticamente del balanceador de carga.

Solo puede agregar servidores en la misma VPC que el balanceador de carga. Para obtener más información, véase **Adición de servidores backend**.

### Precauciones

- Se recomienda que seleccione servidores backend que ejecuten el mismo sistema operativo para facilitar la gestión y el mantenimiento.
- El balanceador de carga comprueba el estado de cada servidor agregado al grupo de servidores backend asociado si ha configurado la comprobación del estado para el grupo de servidores backend. Si el servidor backend responde normalmente, el balanceador de carga lo considerará saludable. Si el servidor backend no responde normalmente, el balanceador de carga comprobará periódicamente su estado hasta que el servidor backend se considere saludable.
- Si se detiene o reinicia un servidor backend, las conexiones establecidas con el servidor se desconectarán y los datos que se transmitan a través de estas conexiones se perderán. Para evitar que esto ocurra, configure la función de reintento en los clientes para evitar la pérdida de datos.
- Si habilita las sesiones adhesivas, el tráfico a los servidores backend puede estar desequilibrado. Si esto sucede, deshabilite las sesiones adhesivas y compruebe las solicitudes recibidas por cada servidor backend.

## Restricciones y limitaciones

- Se puede agregar un máximo de 500 servidores backend a un grupo de servidores backend.
- Las reglas de grupo de seguridad entrante deben configurarse para permitir el tráfico a través del puerto de cada servidor backend y puerto de comprobación de estado. Para obtener más información, véase **Reglas de grupos de seguridad**.

## Ponderación del servidor backend

Necesita establecer una ponderación para cada servidor backend en un grupo de servidores backend para recibir solicitudes. Cuanto mayor sea el peso que haya configurado para un servidor backend, más solicitudes recibirá el servidor backend.

Puede establecer un entero de **0** a **100**. Si establece la ponderación de un servidor backend en **0**, las nuevas solicitudes no se encaminarán a este servidor.

Tres algoritmos de balanceo de carga le permiten establecer ponderaciones para servidores backend, como se muestra en la siguiente tabla. Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Algoritmos de balanceo de carga**.

**Tabla 6-1** Ponderaciones del servidor en diferentes algoritmos de balanceo de carga

| Algoritmo de balanceo de carga | Ajuste de ponderación |
| --- | --- |
| Round robin ponderado | ● Si ninguno de los servidores backend tiene una ponderación de 0, el balanceador de carga enruta las solicitudes a los servidores backend en función de sus ponderaciones. Los servidores backend con ponderaciones más altas reciben proporcionalmente más solicitudes.<br>● Si dos servidores backend tienen la misma ponderación, reciben el mismo número de solicitudes. |
| Planificación por menor número de conexiones y ponderación (weighted least connections) | ● Si ninguno de los servidores backend tiene una ponderación de 0, el balanceador de carga calcula la carga de cada servidor backend usando la fórmula (Overhead = Número de conexiones actuales/ponderación del servidor backend).<br>● El balanceador de carga enruta las solicitudes al servidor backend con la sobrecarga más baja. |
| Hash de IP de origen | ● Si ninguno de los servidores backend tiene una ponderación de 0, las solicitudes del mismo cliente se enrutan al mismo servidor backend dentro de un período de tiempo.<br>● Si la ponderación de un servidor backend es 0, no se enrutan solicitudes a este servidor backend. |

# 6.2 Reglas de grupos de seguridad

Para garantizar las comunicaciones normales entre el balanceador de carga y los servidores backend, debe comprobar las reglas de grupo de seguridad y las reglas de ACL de red configuradas para los servidores backend.

Cuando los servidores backend reciben solicitudes del balanceador de carga, las direcciones IP de origen se traducen en 100.125.0.0/16.

- Las reglas de grupo de seguridad deben permitir el tráfico desde 100.125.0.0/16 a los servidores backend. Para obtener más información acerca de cómo configurar reglas de grupo de seguridad, consulte **Configuración de reglas de grupo de seguridad**.
- Las reglas de ACL de red son opcionales para las subredes. Si se configuran reglas de ACL de red para la subred backend del balanceador de carga, las reglas de ACL de red deben permitir el tráfico desde la subred backend del balanceador de carga a los servidores backend. Para obtener más información acerca de cómo configurar estas reglas, consulte **Configuración de reglas de ACL de red**.

NOTA

Si **Transfer Client IP Address** está habilitado para los oyentes TCP o UDP, las reglas de ACL de red y las reglas de grupo de seguridad no tendrán efecto. Puede usar el control de acceso para limitar qué direcciones IP pueden acceder al oyente. Para aprender a configurar el **control de acceso**.

## Restricciones y limitaciones

- Si la comprobación de estado está habilitada para un grupo de servidores backend, las reglas del grupo de seguridad deben permitir el tráfico desde el puerto de comprobación de estado a través del protocolo de comprobación de estado.
- Si UDP se utiliza para la comprobación de estado, debe haber una regla que permita el tráfico ICMP. Si no existe tal regla, no se puede comprobar el estado de los servidores backend.

## Configuración de reglas de grupo de seguridad

Si no tiene las VPC al crear un servidor, el sistema crea automáticamente una para usted. Las reglas de grupo de seguridad predeterminadas solo permiten comunicaciones entre los servidores de la VPC. Para asegurarse de que el balanceador de carga puede comunicarse con estos servidores tanto a través del puerto frontend como del puerto de comprobación de estado, configure las reglas entrantes para los grupos de seguridad que contienen estos servidores.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. En **Compute**, haga clic en **Elastic Cloud Server**.
4. En la página **Elastic Cloud Server**, haga clic en el nombre del ECS que se ha agregado a un grupo de servidores backend.

   Se mostrará la página que proporciona los detalles del ECS.
5. Haga clic en **Security Groups**, busque el grupo de seguridad y vea las reglas del grupo de seguridad.
6. Haga clic en el ID de una regla o **Modify Security Group Rule** de grupo de seguridad. Se muestra la página de detalles del grupo de seguridad.
7. En la página de ficha **Inbound Rules**, haga clic en **Add Rule**. Configurar una regla de entrada basada en **Tabla 6-2**.

**Tabla 6-2** Reglas de grupos de seguridad

| Protocolo backend | Política | Protocolo & Puerto | Dirección IP de origen |
|---|---|---|---|
| HTTP | Permitir | **Protocol**: TCP<br>**Port**: el puerto utilizado por el servidor backend y el puerto de comprobación de estado | 100.125.0.0/16 |
| TCP | Permitir | **Protocol**: TCP<br>**Port**: puerto de comprobación de estado | 100.125.0.0/16 |
| UDP | Permitir | **Protocol**: UDP e ICMP<br>**Port**: puerto de comprobación de estado | 100.125.0.0/16 |

8. Haga clic en **OK**.

## Configuración de reglas de ACL de red

Para controlar el tráfico dentro y fuera de una subred, puede asociar una ACL de red a la subred. Las reglas de ACL de red controlan el acceso a las subredes y agregan una capa adicional de defensa a las subredes. Las reglas de ACL de red predeterminadas rechazan todo el tráfico entrante y saliente. Si la subred de un balanceador de carga o de los servidores backend asociados tiene un ACL de red asociado, el balanceador de carga no puede recibir tráfico de Internet ni enrutar tráfico a servidores backend, y los servidores backend no pueden recibir tráfico ni responder al balanceador de carga.

Configure una regla de ACL de red entrante para permitir el acceso desde 100.125.0.0/16.

ELB traduce las direcciones IP públicas utilizadas para acceder a servidores backend en direcciones IP privadas en 100.125.0.0/16. No puede configurar reglas para evitar que las direcciones IP públicas accedan a los servidores backend.

**NOTA**

Las reglas de ACL de red configuradas para la subred de fondo del balanceador de carga no restringirán el tráfico de los clientes al balanceador de carga. Si estas reglas están configuradas, los clientes pueden acceder directamente al balanceador de carga. Para controlar el acceso al balanceador de carga, configure el control de acceso para todos los oyentes agregados al balanceador de carga

Para obtener más información, véase **Control de acceso**.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

3. Pase el cursor sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Network ACLs**.
5. En la lista de ACL de red, haga clic en el nombre del ACL de red para cambiar a la página que muestra sus detalles.
6. En la ficha **Inbound Rules** o **Outbound Rules**, haga clic en **Add Rule** para agregar una regla de entrada o de salida.
   - **Action**: Seleccione **Allow**.
   - **Protocol**: El protocolo debe ser el mismo que el protocolo backend.
   - **Source**: Póngalo en **100.125.0.0/16**.
   - **Source Port Range**: Seleccione un rango de puertos.
   - **Destination**: Ingrese una dirección de destino permitida en esta dirección. El valor predeterminado es **0.0.0.0/0**, que indica que se permite el tráfico de todas las direcciones IP.
   - **Destination Port Range**: Seleccione un rango de puertos.
   - (Opcional) **Description**: Describa la regla de ACL de red.
7. Haga clic en **OK**.

# 6.3 Gestión de servidores backend

## 6.3.1 Adición de servidores backend

### Escenario

Puede agregar servidores backend a un grupo de servidores backend para procesar las solicitudes de los clientes.

Cuando utilice ELB para enrutar solicitudes, asegúrese de que al menos un servidor backend se esté ejecutando correctamente y pueda recibir solicitudes enrutadas por el balanceador de carga.

Después de que un servidor backend se desvincule de un balanceador de carga, el servidor backend no recibe solicitudes enviadas por el balanceador de carga, pero el servidor backend se desvincula del balanceador de carga. Puede agregar el servidor backend al grupo de servidores backend de nuevo cuando aumente el tráfico o se necesite mejorar la confiabilidad.

### Restricciones y limitaciones

Solo se pueden agregar servidores en la misma VPC que el balanceador de carga.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
1. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
2. Cambie a la página de pestaña **Backend Servers** y haga clic en **Add** a la derecha.
3. Busque servidores backend con palabras clave especificadas.
4. Especifique las ponderaciones y puertos para los servidores backend y haga clic en **Finish**.

   Los puertos de servidor backend se pueden establecer por lotes.

## 6.3.2 Consulta de servidores backend

### Escenario

Puede ver los servidores backend que se han agregado a un grupo de servidores backend, incluidos su estado, direcciones IP privadas, resultados de comprobación de estado, ponderaciones y puertos.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Backend Servers**.
7. En la lista de servidores backend, vea los servidores backend.

## 6.3.3 Extracción de servidores backend

### Escenario

Puede quitar un servidor backend que ya no sea necesario de un grupo de servidores backend.

Una vez que se quita un servidor backend, se desvincula del balanceador de carga y ya no recibirá solicitudes del balanceador de carga. El servidor backend aún existe. Puede agregar el servidor backend al grupo de servidores backend de nuevo cuando aumente el tráfico o se necesite mejorar la confiabilidad.

### Notas

Después de quitar el servidor backend, las solicitudes siguen siendo enviadas a él. Esto se debe a que se establece una conexión persistente entre el balanceador de carga y el servidor backend y las solicitudes se enrutan a este servidor hasta que se agote el tiempo de espera de la conexión de TCP.

Si no se transmiten datos a través de esta conexión de TCP después de que se agote el tiempo, ELB desconecta la conexión.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Backend Servers**.
7. Seleccione los servidores backend que desea quitar y haga clic en **Remove** encima de la lista de servidores backend.
8. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

## 6.3.4 Cambio de las ponderaciones del servidor backend

### Escenarios

Puede cambiar las ponderaciones especificadas para los servidores backend en función de su capacidad para procesar solicitudes.

### Restricciones y limitaciones

- Puede establecer un entero de **0** a **100**. Si establece la ponderación de un servidor backend en **0**, las nuevas solicitudes no se encaminarán a este servidor.
- Las ponderaciones solo se pueden especificar cuando se selecciona round robin ponderado, conexiones mínimas ponderadas o hash IP de origen como algoritmo de balanceo de carga. Para obtener más información acerca de los algoritmos de balanceo de carga, consulte **Ponderación del servidor backend**.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **Backend Server Groups**.
5. En la página **Backend Server Groups**, haga clic en el nombre del grupo de servidores backend.
6. Cambie a la página de la ficha **Backend Servers** y haga clic en **Backend Servers**.
7. Seleccione los servidores backend y haga clic en **Modify Weight** encima de la lista de servidores backend.
8. En el cuadro de diálogo que se muestra, modifique las ponderaciones según lo necesite.
   - Cambiar la ponderación de un único servidor backend: Establezca la ponderación en la columna **Weight**.
   - Cambiar las ponderaciones de varios servidores backend: Establezca la ponderación junto a **Batch Modify Weights** y haga clic en **OK**.

   NOTA

   Puede cambiar las ponderaciones de varios servidores backend a **0** para que no reciban solicitudes del balanceador de carga.
9. Haga clic en **OK**.

# 7 Certificado

## 7.1 Introducción a los certificados

ELB admite dos tipos de certificados. Si necesita un oyente de HTTPS, debe vincular un certificado de servidor a él. Para habilitar la autenticación mutua, también debe vincular un certificado de CA al oyente.

- **Server certificate**: utilizado para las negociaciones de protocolo de enlace SSL si se utiliza un HTTPS oyente. Se requieren tanto el contenido del certificado como la clave privada.
- **CA certificate**: emitido por una entidad emisora de certificados (CA) y utilizado para verificar el emisor del certificado. Si se requiere autenticación mutua HTTPS, las conexiones HTTPS solo se pueden establecer cuando el cliente proporciona un certificado emitido por un CA específico.

NOTA

SSL Certificate Manager (SCM) le permite comprar un certificado de Huawei Cloud o cargar sus propios certificados para una gestión más sencilla.

### Precauciones

- Un certificado puede ser utilizado por varios balanceadores de carga, pero solo necesita ser cargado en cada balanceador de carga una vez.
- Si se utiliza un certificado para SNI, puede especificar varios nombres de dominio para el certificado y los nombres de dominio deben ser los mismos que los del certificado.
- Para cada tipo de certificado, un oyente solo puede tener un certificado por defecto, pero un certificado puede estar vinculado a más de un oyente. Si el SNI está habilitado para el oyente, se pueden enlazar varios certificados de servidor.
- Sólo se admiten los certificados originales. Es decir, no puede cifrar sus certificados.
- No es necesario configurar certificados tanto para los balanceadores de carga compartidos como para los servidores backend asociados. Si configura un certificado para servidores backend, HTTPS oyentes no se pueden agregar al balanceador de carga. En este caso, puede agregar un oyente TCP para transmitir de forma transparente el tráfico HTTPS a los servidores backend. Esta restricción no se aplica a los balanceadores de carga dedicados.

- Puede utilizar certificados autofirmados. Sin embargo, tenga en cuenta que los certificados autofirmados plantean riesgos de seguridad. Por lo tanto, se recomienda utilizar certificados emitidos por terceros.
- ELB admite certificados solo en formato PEM. Si tiene un certificado en cualquier otro formato, debe convertirlo en un certificado codificado por PEM.
- Si un certificado ha caducado, debe reemplazarlo o eliminarlo manualmente.

# 7.2 Certificado y formato de clave privada

## Formato de certificado

Puede copiar y pegar el cuerpo del certificado para crear un certificado o cargarlo directamente.

Un certificado emitido por Root CA es único y no se requieren certificados adicionales. El sitio configurado se considera fiable por los dispositivos de acceso, como un navegador.

El cuerpo del servidor y los certificados de CA deben cumplir los requisitos que se describen a continuación.

- El contenido comienza con **-----BEGIN CERTIFICATE-----** y termina con **-----END CERTIFICATE-----**.
- Cada fila contiene 64 caracteres excepto la última fila.
- No hay filas vacías.

A continuación se presenta un ejemplo:

```
-----BEGIN CERTIFICATE-----
MIIDIjCCAougAwIBAgIJALV96mEtVF4EMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNV
BAYTAnh4MQswCQYDVQQIEwJ4eDELMAkGA1UEBxMCeHgxCzAJBgNVBAoTAnh4MQsw
CQYDVQQLEwJ4eDELMAkGA1UEAxMCeHgxGjAYBgkqhkiG9w0BCQEWC3h4eEAxNjMu
Y29tMB4XDTE3MTExMzAyMjYxM1oXDTIwMTExMjAyMjYxM1owajELMAkGA1UEBhMC
eHgxCzAJBgNVBAgTAnh4MQswCQYDVQQHEwJ4eDELMAkGA1UEChMCeHgxCzAJBgNV
BAsTAnh4MQswCQYDVQQDEwJ4eDEaMBgGCSqGSIb3DQEJARYLeHh4QDE2My5jb20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMU832iM+d3FILgTWmpZBUoYcIWV
cAAYE7FsZ9LNerOyjJpyi256oypdBvGs9JAUBN5WaFk81UQx29wAyNixX+bKa0DB
WpUDqr84V1f9vdQc75v9WoujcnlKszzpV6qePPC7igJJpu4QOI362BrWzJCYQbg4
Uzo1KYBhLFxl0TovAgMBAAGjgc8wgcwwHQYDVR0OBBYEFMbTvDyvE2KsRy9zPq/J
WOjovG+WMIGcBgNVHSMEgZQwgZGAFMbTvDyvE2KsRy9zPq/JWOjovG+WoW6kbDBq
MQswCQYDVQQGEwJ4eDELMAkGA1UECBMCeHgxCzAJBgNVBAcTAnh4MQswCQYDVQQK
EwJ4eDELMAkGA1UECxMCeHgxCzAJBgNVBAMTAnh4MRowGAYJKoZIhvcNAQkBFgt4
eHhAMTYzLmNvbYIJALV96mEtVF4EMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
BQADgYEAASkC/1iwiALa2RU3YCxqZFEEsZZvQxikrDkDbFeoa6Tk49Fnb1f7FCW6
PTtY3HPWl5ygsMsSy0Fi3xp3jmuIwzJhcQ3tcK5gC99HWp6Kw37RL8WoB8GWFU0Q
4tHLOjBIxkZROPRhH+zMIrqUexv6fsb3NWKhnlfh1Mj5wQE4Ldo=
-----END CERTIFICATE-----
```

## Formato de clave privada

Al crear un certificado de servidor, también debe cargar la clave privada del certificado. Puede copiar y pegar el contenido de la clave privada o cargar directamente la clave privada en el formato requerido.

Las claves privadas deben estar descifradas y cumplir con los siguientes requisitos:

- El valor debe estar en formato PEM.
  - El contenido debe comenzar con **-----BEGIN RSA PRIVATE KEY-----** y **-----END RSA PRIVATE KEY-----**.

  - El contenido debe comenzar con **-----BEGIN EC PRIVATE KEY-----** y terminar con **-----END EC PRIVATE KEY-----**.
- No hay filas vacías. Cada fila debe contener 64 caracteres excepto la última fila.

A continuación se presenta un ejemplo:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDFPN9ojPndxSC4E1pqWQVKGHCFlXAAGBOxbGfSzXqzsoyacotu
eqMqXQbxrPSQFATeVmhZPNVEMdvcAMjYsV/mymtAwVqVA6q/OFdX/b3UHO+b/VqL
o3J5SrM86Veqnjzwu4oCSabuEDiN+tga1syQmEG4OFM6NSmAYSxcZdE6LwIDAQAB
AoGBAJvLzJCyIsCJcKHWL6onbSUtDtyFwPViD1QrVAtQYabF14g8CGUZG/9fgheu
TXPtTDcvu7cZdUArvgYW3I9F9IBb2lmF3a44xfiAKdDhzr4DK/vQhvHPuuTeZA41
r2zp8Cu+Bp40pSxmoAOK3B0/peZAka01Ju7c7ZChDWrxleHZAkEA/6dcaWHotfGS
eW5YLbSms3f0m0GH38nRl7oxyCW6yMIDkFHURVMBKWlOhrcuGo8u0nTMi5IH9gRg
5bH8XcujlQJBAMWBQgzCHyoSeryD3TFieXIFzgDBw6Ve5hyMjUtjvgdVKoxRPvpO
kclc39QHP6Dm2wrXXHEej+9RILxBZCVQNbMCQQC42i+Ut0nHvPuXN/UkXzomDHde
h1ySsOAO4H+8Y6OSI87l3HUrByCQ7stX1z3L0HofjHqV9Koy9emGTFLZEzSdAkB7
Ei6cUKKmztkYe3rr+RcATEmwAw3tEJOHmrW5ErApVZKr2TzLMQZ7WZpIPzQRCYnY
2ZZLDuZWFFG3vW+wKKktAkAaQ5GNzbwkRLpXF1FZFuNF7erxypzstbUmU/31b7tS
i5LmxTGKL/xRYtZEHjya4Ikkkgt40q1MrUsgIYbFYMf2
-----END RSA PRIVATE KEY-----
```

# 7.3 Conversión de formatos de certificado

## Escenarios

ELB admite certificados solo en formato PEM. Si tiene un certificado en cualquier otro formato, debe convertirlo en un certificado codificado por PEM. Hay algunos métodos comunes para convertir un certificado de cualquier otro formato a PEM.

## De DER a PEM

El formato DER se utiliza generalmente en una plataforma Java.

Ejecute el siguiente comando para convertir el formato de certificado:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

Ejecute el siguiente comando para convertir el formato de clave privada:

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

## De P7B a PEM

El formato P7B es generalmente utilizado por Windows Server y Tomcat.

Ejecute el siguiente comando para convertir el formato de certificado:

```
openssl pkcs7 -print_certs -in incertificate.p7b -out outcertificate.cer
```

## De PFX a PEM

El formato PFX es generalmente utilizado por Windows Server.

Ejecute el siguiente comando para convertir el formato de certificado:

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

Ejecute el siguiente comando para convertir el formato de clave privada:

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

# 7.4 Adición de un certificado

## Escenarios

Para habilitar la autenticación para proteger la transmisión de datos a través de HTTPS, ELB le permite vincular certificados a los oyentes HTTPS de un balanceador de carga.

- Certificado de servidor: Puede comprar un certificado de SSL Certificate Manager (SCM) o cargar sus propios certificados.
- Certificado de CA: solo puede cargar sus propios certificados de CA.

NOTA

Si desea utilizar el mismo certificado en dos regiones, debe crear un certificado en cada región.

## Adición de un certificado de servidor

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Certificates**.
5. Haga clic en **Add Certificate** en la esquina superior derecha y establezca los parámetros haciendo referencia a **Tabla 7-1**.

**Tabla 7-1** Parámetros del certificado del servidor

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Certificate Type | Especifica el tipo de certificado.<br>● **Server certificate**: utilizado para las negociaciones de protocolo de enlace SSL si se utiliza un HTTPS oyente. Se requieren tanto el contenido del certificado como la clave privada.<br>● **CA certificate**: emitido por una entidad emisora de certificados (CA) y utilizado para verificar el emisor del certificado. Si se requiere autenticación mutua HTTPS, las conexiones HTTPS solo se pueden establecer cuando el cliente proporciona un certificado emitido por un CA específico. | Server certificate |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Source | Especifica el origen de un certificado. Puede comprar un certificado de SCM o cargar sus propios certificados.<br>● **SCM certificate**: certificado de servidor proporcionado por SCM. Necesita comprar un certificado o cargar su propio certificado en la consola SCM.<br>● **Your certificate**: Debe cargar el contenido del certificado y la clave privada de su propio certificado en la consola de ELB.<br>**NOTA**<br>Se recomienda utilizar SCM para gestionar sus certificados. | SCM certificate |
| Certificate | Este parámetro solo está disponible para certificados SCM.<br>Puede seleccionar certificados proporcionados por SCM. | - |
| Certificate Name | Especifica el nombre del certificado.<br>Este parámetro solo está disponible para sus certificados. | - |
| Enterprise Project | Especifica un proyecto de empresa mediante el cual los recursos de nube y los miembros se gestionan de forma centralizada. | default |
| Certificate Content | Especifica el contenido de un certificado. Este parámetro solo está disponible para sus certificados.<br>El contenido debe estar en formato PEM.<br>Haga clic en **Upload** y seleccione un certificado. Asegúrese de que su navegador es la última versión.<br>El formato se muestra a continuación:<br>`-----BEGIN CERTIFICATE-----`<br>`Base64-encoded certificate`<br>`-----END CERTIFICATE-----` | - |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Private Key | Especifica la clave privada de un certificado. Este parámetro solo está disponible para sus certificados.<br>Haga clic en **Upload** y seleccione una clave privada. Asegúrese de que su navegador es la última versión.<br>El valor debe ser una clave privada no cifrada. El formato se muestra a continuación:<br>`-----BEGIN PRIVATE KEY-----`<br>`[key]`<br>`-----END PRIVATE KEY-----` | - |
| Domain Name | El nombre de dominio debe especificarse si el certificado está destinado a SNI.<br>Solo se puede especificar un nombre de dominio para cada certificado, y el nombre de dominio debe ser el mismo que en el certificado. | - |
| Description | (Opcional) Proporciona información adicional sobre el certificado. | - |

## Adición de un certificado de CA

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Certificates**.
5. Haga clic en **Add Certificate** en la esquina superior derecha y establezca los parámetros haciendo referencia a **Tabla 7-2**.

**Tabla 7-2** Parámetros del certificado de CA

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Certificate Type | Especifica el tipo de certificado.<br>● **Server certificate**: utilizado para las negociaciones de protocolo de enlace SSL si se utiliza un HTTPS oyente. Se requieren tanto el contenido del certificado como la clave privada.<br>● **CA certificate**: emitido por una entidad emisora de certificados (CA) y utilizado para verificar el emisor del certificado. Si se requiere autenticación mutua HTTPS, las conexiones HTTPS solo se pueden establecer cuando el cliente proporciona un certificado emitido por un CA específico. | CA certificate |
| Certificate Name | Especifica el nombre del certificado de CA. | - |
| Enterprise Project | Especifica un proyecto de empresa mediante el cual los recursos de nube y los miembros se gestionan de forma centralizada. | default |
| Certificate Content | El contenido debe estar en formato PEM.<br>Haga clic en **Upload** y seleccione un certificado. Asegúrese de que su navegador es la última versión.<br>El formato se muestra a continuación:<br>`-----BEGIN CERTIFICATE-----`<br>`Base64-encoded certificate`<br>`-----END CERTIFICATE-----` | - |
| Description | (Opcional) Proporciona información adicional sobre el certificado. | - |

6. Haga clic en **OK**.

# 7.5 Eliminación de un certificado

## Escenarios

Si ya no se necesita un certificado, puede eliminarlo en la consola de ELB.

## Restricciones

No se puede eliminar un certificado enlazado a un oyente HTTPS. En primer lugar, desvincule el certificado del oyente haciendo referencia a **Sustitución de un certificado**.

### Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Certificates**.
5. Busque el certificado y haga clic en **Delete** en la columna **Operation**.
6. Haga clic en **Yes**.

## 7.6 Vinculación de un oyente y sustitución del certificado enlazado a un oyente

### Escenarios

Necesita vincular un certificado cuando agrega un oyente HTTPS a un balanceador de carga. Si el certificado utilizado por un oyente ha caducado o necesita ser reemplazado por otras razones, puede reemplazar el certificado en la pestaña **Listeners**.

Si el certificado también es utilizado por otros servicios como WAF, reemplace el certificado en todos estos servicios para evitar la indisponibilidad del servicio.

NOTA

La sustitución de certificados y claves privadas no afecta a las aplicaciones.

### Requisitos previos

Ha creado un certificado siguiendo las instrucciones en **Adición de un certificado**.

### Vinculación de un certificado

Puede enlazar certificados cuando agrega un oyente HTTPS. Para obtener más información, véase **Adición de un oyente de HTTPS**.

### Sustitución de un certificado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en la ficha **Listeners**, busque el oyente y haga clic en **Edit** en la columna **Operation**.

6. Seleccione un certificado de servidor.
7. Haga clic en **OK** en el cuadro de diálogo **Edit**.

# 7.7 Reemplazar el certificado vinculado a diferentes oyentes

## Escenario

Si el certificado enlazado a diferentes oyentes ha caducado o necesita ser reemplazado por otras razones, puede reemplazar el certificado modificándolo en la página **Certificates**.

NOTA

La sustitución del certificado y las claves privadas no afecta a las aplicaciones.

## Restricciones

- Solo los oyentes de HTTPS requieren certificados.
- El nuevo certificado entra en vigor inmediatamente. El certificado antiguo se utiliza para conexiones establecidas, y el nuevo se utiliza para nuevas conexiones.
- SSL Certificate Manager (SCM) le permite comprar un certificado de Huawei Cloud o cargar sus propios certificados para una gestión más sencilla.

## Modificación de un certificado

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Certificates**.
5. Busque el certificado y haga clic en **Modify** en la columna **Operation**.
6. Modifique los parámetros según sea necesario.
7. Confirme la información y haga clic en **OK**.

# 7.8 Consulta de oyentes por certificado

## Escenarios

Es necesario ver rápidamente los detalles de los oyentes a los que está enlazado un certificado.

## Procedimiento

1. Inicie sesión en la consola de gestión.

2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Certificates**.
5. En la lista de certificados, haga clic en el nombre de oyente en la columna **Listener (Frontend Protocol/Port)** para ver sus detalles.

   Si hay más de 5 oyentes, no se muestra ningún oyente en la columna **Listener (Frontend Protocol/Port)**. Haga clic en **View All**. En la página mostrada, haga clic en **Listeners**, busque el oyente y haga clic en su nombre para ver los detalles.

# 8 Control de acceso

## 8.1 Control de acceso

El control de acceso le permite agregar una lista blanca o una lista negra para especificar direcciones IP que están permitidas o denegadas para acceder a un oyente. Una lista blanca permite que las direcciones IP especificadas accedan al oyente, mientras que una lista negra deniega el acceso desde las direcciones IP especificadas.

**AVISO**

- Agregar la lista blanca o la lista negra puede causar riesgos.
  - Una vez establecida la lista blanca, solo las direcciones IP especificadas en la lista blanca pueden acceder al oyente.
  - Una vez establecida la lista negra, las direcciones IP especificadas en la lista negra no pueden acceder al oyente.
- Las listas blancas y las listas negras no entran en conflicto con las reglas del grupo de seguridad entrante. Las listas blancas definen las direcciones IP a las que se les permite acceder a los oyentes, mientras que las listas negras especifican las direcciones IP a las que se les deniega el acceso a los oyentes. Las reglas de grupo de seguridad entrantes controlan el acceso a los servidores backend especificando el protocolo, los puertos y las direcciones IP.
- El control de acceso no restringe el comando ping. Todavía puede hacer ping a los servidores backend desde las direcciones IP restringidas.
  - Para hacer ping a la dirección IP de un balanceador de carga compartido, debe agregar un oyente y asociar un servidor backend a él.
  - Para hacer ping a la dirección IP de un balanceador de carga dedicado, solo necesita agregarle un oyente.
- Las políticas de control de acceso solo tienen efecto para las nuevas conexiones, pero no para las conexiones que se hayan establecido. Si se configura una lista blanca para un oyente pero las direcciones IP que no están en la lista blanca pueden acceder al servidor backend asociado con el oyente, una posible razón es que se establece una conexión persistente entre el cliente y el servidor backend. Para impedir que las direcciones IP que no están en la lista blanca accedan al oyente, es necesario desconectar la conexión persistente entre el cliente y el servidor backend.

## Configuración del control de acceso

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Puede configurar el control de acceso para un oyente de cualquiera de las siguientes maneras:
   - En la página **Listeners**, busque el oyente y haga clic en **Configure** en la columna **Access Control**.
   - Haga clic en el nombre del oyente de destino. En la página **Summary**, haga clic en **Configure** a la derecha de **Access Control**.
6. En el cuadro de diálogo **Configure Access Control** que se muestra, configure los parámetros como se muestra en **Tabla 8-1**.

**Tabla 8-1** Descripción del parámetro

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Control de acceso | Especifica cómo se controla el acceso al oyente. Hay tres opciones disponibles:<br>● **All IP addresses**: Todas las direcciones IP pueden acceder al oyente.<br>● **Whitelist**: Solo las direcciones IP del grupo de direcciones IP pueden acceder al oyente.<br>● **Blacklist**: las direcciones IP del grupo de direcciones IP no pueden acceder al oyente. | Blacklist |
| IP Address Group | Especifica el grupo de direcciones IP asociado a una lista blanca o negra. Si no hay un grupo de direcciones IP, cree uno primero. Para obtener más información, consulte **Descripción del grupo de direcciones IP**. | ipGroup-b2 |
| Control de acceso | Si ha configurado **Access Control** en **Whitelist** o **Blacklist** puede activar o desactivar el control de acceso.<br>● Solo después de habilitar el control de acceso, la lista blanca o la lista negra entrará en vigor.<br>● Si deshabilita el control de acceso, la lista blanca o la lista negra no surte efecto. | N/A |

7. Haga clic en **OK**.

# 8.2 Gestión de grupos de direcciones IP

## 8.2.1 Creación de un grupo de direcciones IP

### Descripción del grupo de direcciones IP

Un grupo de direcciones IP es una colección de direcciones IP que puede utilizar para gestionar direcciones IP con los mismos requisitos de seguridad o cuyos requisitos de seguridad cambian con frecuencia.

ELB le permite usar una lista blanca o una lista negra para el control de acceso. Si desea configurar una política de **access control**, debe seleccionar un grupo de direcciones IP.

- **Whitelist**: Solo las direcciones IP del grupo de direcciones IP pueden acceder al oyente. Si el grupo de direcciones IP no contiene ninguna dirección IP y ha seleccionado la lista blanca para el control de acceso, ninguna dirección IP puede acceder al oyente.
- **Blacklist**: Las direcciones IP del grupo de direcciones IP son denegadas para acceder al oyente. Si el grupo de direcciones IP no contiene ninguna dirección IP y ha seleccionado la lista negra para el control de acceso, todas las direcciones IP pueden acceder al oyente.

## Restricciones

- De forma predeterminada, puede crear un máximo de 50 grupos de direcciones IP.
- Un grupo de direcciones IP se puede vincular con un máximo de 50 oyentes.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **IP Address Groups**.
5. En la página mostrada, haga clic en **Create IP Address Group**.
6. Configure los parámetros basados en **Tabla 8-2**.

**Tabla 8-2** Parámetros necesarios para crear un grupo de direcciones IP

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Name | Especifica el nombre del grupo de direcciones IP. | ipGroup-01 |
| Enterprise Project | Especifica un proyecto de empresa mediante el cual los recursos de nube y los miembros se gestionan de forma centralizada. Para obtener más información, consulte la **Guía del usuario de Enterprise Management**. | - |
| IP Addresses | Especifica direcciones IP IPv4 o IPv6 o bloques CIDR que se agregan a la lista blanca o la lista negra para el control de acceso.<br>● Cada línea debe contener una dirección IP o un bloque CIDR y terminar con un salto de línea.<br>● Cada dirección IP o bloque CIDR puede incluir una descripción con una barra vertical (\|) separada, por ejemplo, 192.168.10.10 \| ECS01. La descripción tiene una longitud de 0 a 255 caracteres y no puede contener corchetes angulares (<>).<br>● Puede agregar un máximo de 300 direcciones IP o bloques CIDR en cada grupo de direcciones IP. | 10.168.2.24<br>10.168.16.0/24 |

| Parámetro | Descripción | Valor de ejemplo |
| --- | --- | --- |
| Description | Proporciona información adicional sobre el grupo de direcciones IP. | - |

7. Haga clic en **OK**.

# 8.2.2 Consulta de los detalles de un grupo de direcciones IP

## Escenarios

Esta sección describe cómo puede ver información acerca de un grupo de direcciones IP, incluidos:

- Nombre, ID y tiempo de creación
- Direcciones IP y bloques CIDR
- Oyentes asociados

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **IP Address Groups**.
5. En la página **IP Address Groups**, haga clic en el nombre del grupo de direcciones de destino.
6. Consulta de información básica sobre un grupo de direcciones IP.
   a. En la ficha **IP Addresses**, vea las direcciones IP.
   b. En la ficha **Associated Listeners**, vea los oyentes asociados al grupo de direcciones IP.

# 8.2.3 Gestión de direcciones IP en un grupo de direcciones IP

Después de crear un grupo de direcciones IP, puede gestionar las direcciones IP en un grupo de direcciones IP según sea necesario:

- **Adición de direcciones IP**
- **Cambio de direcciones IP**
- **Eliminación de una dirección IP**

## Restricciones

Las direcciones IP pueden estar en los siguientes formatos:

- Cada línea debe contener una dirección IP o un bloque CIDR y terminar con un salto de línea.
- Cada dirección IP o bloque CIDR puede incluir una descripción con una barra vertical (|) separada, por ejemplo, 192.168.10.10 | ECS01. La descripción tiene una longitud de 0 a 255 caracteres y no puede contener corchetes angulares (<>).
- Puede agregar un máximo de 300 direcciones IP o bloques CIDR en cada grupo de direcciones IP.

## Adición de direcciones IP

Después de crear un grupo de direcciones IP, puede agregar direcciones IP a un grupo de direcciones IP.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **IP Address Groups**.
5. En la página **IP Address Groups**, haga clic en el nombre del grupo de direcciones de destino.
6. En la parte inferior de la página mostrada, elija la ficha **IP Addresses** y haga clic en **Add IP Addresses**.
7. En la página **Add IP Addresses**, agregue direcciones IP.
8. Haga clic en **OK**.

## Cambio de direcciones IP

Puede realizar los siguientes pasos para cambiar todas las direcciones IP de un grupo de direcciones IP:

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **IP Address Groups**.
5. En la página **IP Address Groups**, puede:
   a. Modificar la información básica y cambie las direcciones IP de un grupo de direcciones IP:
      i. Busque el grupo de direcciones de destino y haga clic en **Modify** en la columna **Operation**.
      ii. Puede modificar el nombre y la descripción de un grupo de direcciones IP y cambiar todas sus direcciones IP.

iii. Haga clic en **OK**.

b. Solo cambiar las direcciones IP:

i. Haga clic en el nombre del grupo de direcciones IP de destino.

ii. En la parte inferior de la página mostrada, elija la ficha **IP Addresses** y haga clic en **Change IP Address**.

iii. Cambie las direcciones IP según lo necesite.

iv. Haga clic en **OK**.

### Eliminación de una dirección IP

Si desea eliminar las direcciones IP por lotes de un grupo de direcciones IP, consulte **Cambio de direcciones IP**.

Para eliminar una dirección IP de un grupo de direcciones IP, realice las siguientes operaciones:

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **IP Address Groups**.
5. En la página **IP Address Groups**, haga clic en el nombre del grupo de direcciones de destino.
6. En la lista de direcciones IP, busque la dirección IP que desea eliminar y haga clic en **Delete** en la columna **Operation**.

   Aparecerá en pantalla un cuadro de diálogo de confirmación.
7. Confirme la información y haga clic en **Yes**.

## 8.2.4 Eliminación de un grupo de direcciones IP

### Escenarios

Si ya no necesita un grupo de direcciones IP, puede eliminarlo. En esta sección se describe cómo eliminar un grupo de direcciones IP.

### Restricciones

Un grupo de direcciones IP que se ha utilizado para controlar el acceso a un oyente no se puede eliminar. Puede ver los oyentes asociados a un grupo de direcciones IP haciendo referencia a **Consulta de los detalles de un grupo de direcciones IP**. Para obtener más información acerca de cómo desasociar un grupo de direcciones IP de un oyente, consulte **Configuración del control de acceso**.

### Procedimiento

1. Inicie sesión en la consola de gestión.

2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. En el panel de navegación de la izquierda, elija **Elastic Load Balance** > **IP Address Groups**.
5. En la página **IP Address Groups**, busque el grupo de direcciones IP y haga clic en **Delete** en la columna **Operation**.
6. Haga clic en **Yes**.

# 9 Etiqueta

## Escenarios

Si tiene una gran cantidad de recursos en la nube, puede agregar diferentes etiquetas a los recursos para identificarlos rápidamente y usar estas etiquetas para gestionar fácilmente sus recursos.

## Adición de una etiqueta a un balanceador de carga

Puede agregar una etiqueta a un balanceador de carga con el siguiente método:

- Agregue una etiqueta cuando cree un balanceador de carga.

  Para obtener más información, consulte **Creación de un balanceador de carga dedicado** y **Creación de un balanceador de carga compartido**.
- Agregue una etiqueta a un balanceador de carga existente.
  a. Inicie sesión en la consola de gestión.
  b. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
  c. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
  d. Busque el balanceador de carga y haga clic en su nombre.
  e. En **Tags**, haga clic en **Add Tag**.
  f. En el cuadro de diálogo **Add Tag**, escriba una clave y un valor de etiqueta y haga clic en **OK**.

  NOTA

  - Se puede agregar un máximo de 10 etiquetas a un balanceador de carga.
  - Cada etiqueta es un par clave-valor, y la clave de etiqueta es única.

## Agregar una etiqueta a un oyente

Para agregar una etiqueta a un oyente existente, realice los siguientes pasos:

1. Inicie sesión en la consola de gestión.

2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Listeners**, busque el oyente y haga clic en su nombre.
6. En **Tags**, haga clic en **Add Tag**.
7. En el cuadro de diálogo **Add Tag**, escriba una clave y un valor de etiqueta y haga clic en **OK**.

   NOTA

   - Se puede agregar un máximo de 10 etiquetas a un oyente.
   - Cada etiqueta es un par clave-valor, y la clave de etiqueta es única.

## Modificación de una etiqueta

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Tags**, seleccione la etiqueta que desea editar y haga clic en **Edit** en la columna **Operation**. En el cuadro de diálogo **Edit Tag**, cambie el valor de etiqueta.

   NOTA

   La clave de etiqueta no se puede cambiar.
6. Haga clic en **OK**.

Las operaciones para modificar una etiqueta oyente no se detallan aquí. Consulte las operaciones de modificación de una etiqueta de balanceador de carga.

## Eliminación de una etiqueta

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Haga clic en **Tags**, seleccione la etiqueta que desea eliminar y haga clic en **Delete** en la columna **Operation**.
6. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

Las operaciones para eliminar una etiqueta oyente no se detallan aquí. Consulte las operaciones de eliminación de una etiqueta de balanceador de carga.

# 10 Registro de acceso

## Escenarios

ELB registra las solicitudes HTTP y HTTPS recibidas por los balanceadores de carga, incluida la hora en que se envió la solicitud, la dirección IP del cliente, la ruta de la solicitud y la respuesta del servidor. Para habilitar el log de acceso, debe interconectar ELB con LTS y crear un grupo de log y un flujo de log en la consola LTS.

El registro de acceso es compatible con los oyentes de HTTP/HTTPS de balanceadores de carga dedicados y compartidos.

## Configuración de LTS

Para ver los registros de acceso, primero debe configurar LTS siguiendo las instrucciones en la **Guía del usuario de Log Tank Service**.

1. Cree un grupo de log.
   a. Inicie sesión en la consola de gestión.
   b. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
   c. Haga clic en en la esquina superior izquierda y haga **Management & Governance** > **Log Tank Service**.
   d. En el panel de navegación de la izquierda, elija **Log Management**.
   e. Haga clic en **Create Log Group**. En el cuadro de diálogo que se muestra, escriba un nombre para el grupo de log.

      Establezca **Log Retention Duration** según sea necesario.
   f. Haga clic en **OK**.
2. Cree un flujo de log.
   a. En la consola de LTS, haga clic en a la izquierda de un nombre de grupo de log.
   b. Haga clic en **Create Log Stream**. En el cuadro de diálogo que se muestra, escriba un nombre para el flujo de log.

c. Seleccione un proyecto de empresa según sea necesario.
d. Haga clic en **OK**.

## Configuración del registro de acceso

Configurar el registro de acceso en la consola ELB.

1. Pase el ratón sobre  en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
2. Busque el balanceador de carga y haga clic en su nombre.
3. En **Access Logs**, haga clic en **Configure Access Logging**.
4. Habilite el log de acceso y seleccione el grupo de log y el flujo de log que creó.
5. Haga clic en **OK**.

## Consultar logs de acceso

Después de habilitar el registro de acceso, puede obtener detalles sobre las solicitudes enviadas al balanceador de carga.

Hay dos formas de ver los registros de acceso.

- En la consola ELB, haga clic en el nombre del balanceador de carga y haga clic en **Access Logs** para ver los registros.
- (Recomendado) En la consola LTS, haga clic en el nombre del flujo de log correspondiente. En la página mostrada, haga clic en **Real-Time Logs**

Lo siguiente es un log de ejemplo. Para obtener más información sobre los campos del log, consulte **Tabla 10-1**. El formato de log no se puede modificar.

```
$msec $access_log_topic_id [$time_iso8601] $log_ver $remote_addr:$remote_port
$status "$request_method $scheme://$host$router_request_uri $server_protocol"
$request_length $bytes_sent $body_bytes_sent $request_time "$upstream_status"
"$upstream_connect_time" "$upstream_header_time" "$upstream_response_time"
"$upstream_addr" "$http_user_agent" "$http_referer" "$http_x_forwarded_for"
$lb_name $listener_name $listener_id
$pool_name "$member_name" $tenant_id $eip_address:$eip_port "$upstream_addr_priv"
$certificate_id $ssl_protocol $ssl_cipher $sni_domain_name $tcpinfo_rtt
$self_defined_header
```

**Tabla 10-1** Descripción del parámetro

| Parámetro | Descripción | Descripción | Valor de ejemplo |
|---|---|---|---|
| msec | Tiempo en segundos con una resolución de milisegundos | Datos de punto flotante | 1530153091.868 |
| access_log_topic_id | ID de flujo de log | UUID | 04465dfa-640f-4567-8b58-45c9f8bbc23f |
| time_iso8601 | Hora local en el formato estándar ISO 8601 | - | 2018-06-28T10:31:31+08:00 |
| log_ver | Versión de formato de log | Valor fijo: **elb_01** | elb_01 |

| Parámetro | Descripción | Descripción | Valor de ejemplo |
| --- | --- | --- | --- |
| remote_addr: remote_port | Dirección IP y número del puerto del cliente | Registra la dirección IP y el puerto del cliente. | 10.184.30.170:59605 |
| status | Código de estado de HTTP | Registra el código de estado de la solicitud. | 200 |
| request_method scheme://host request_uri server_protocol | *Request method Protocol*:// *Host name: Request URI Request protocol* | • **request_method**: método de solicitud<br>• **scheme**: HTTP o HTTPS<br>• **host**: nombre de host, que puede ser un nombre de dominio o una dirección IP<br>• **request_uri**: indica que el URI nativo iniciado por el navegador sin ninguna modificación no incluye el protocolo y el nombre de host. | POST https://setting1.hicloud.com/AccountServer/IUserInfoMng/stAuth?Version=26400&cVersion=ID_SDK_2.6.4.300 |
| request_length | Longitud de la solicitud recibida del cliente, incluidos el encabezado y el cuerpo | Integer | 295 |
| bytes_sent | Número de bytes enviados al cliente | Integer | 58470080 |
| body_bytes_sent | Número de bytes enviados al cliente (excepto el encabezado de respuesta) | Integer | 58469792 |

| Parámetro | Descripción | Descripción | Valor de ejemplo |
|---|---|---|---|
| request_time | Tiempo de procesamiento de la solicitud en segundos desde el momento en que el balanceador de carga recibe el primer paquete de solicitud del cliente hasta el momento en que el balanceador de carga envía el paquete de respuesta | Datos de punto flotante | 499.769 |
| upstream_status | Código de estado de respuesta devuelto por el servidor backend<br>● Cuando el balanceador de carga intenta reintentar una solicitud, habrá varios códigos de estado de respuesta.<br>● Si la solicitud no se enruta correctamente al servidor backend, se muestra un guion (-) como valor nulo para este campo. | Código de estado HTTP devuelto por el servidor backend al balanceador de carga | 200 or "-, 200", or "502, 502: 200", or "502:" |
| upstream_connect_time | Tiempo necesario para establecer una conexión con el servidor backend, en segundos, con una resolución de milisegundos<br>● Cuando el balanceador de carga intente volver a intentar una solicitud, habrá varios tiempos de conexión.<br>● Si la solicitud no se enruta correctamente al servidor backend, se muestra un guion (-) como valor nulo para este campo. | Datos de punto flotante | 0.008, "-, 0.008", "0.008, 0.005: 0.004", or "0.008:" |

| Parámetro | Descripción | Descripción | Valor de ejemplo |
| --- | --- | --- | --- |
| upstream_header_time | Tiempo necesario para recibir el encabezado de respuesta del servidor backend, en segundos, con una resolución de milisegundos<br>● Cuando el balanceador de carga intenta volver a intentar una solicitud, habrá varios tiempos de respuesta.<br>● Si la solicitud no se enruta correctamente al servidor backend, se muestra un guion (-) como valor nulo para este campo. | Datos de punto flotante | 0.008, "-, 0.008", "0.008, 0.005: 0.004", or "0.008:" |
| upstream_response_time | Tiempo necesario para recibir la respuesta del servidor backend, en segundos, con una resolución de milisegundos<br>● Cuando el balanceador de carga intenta volver a intentar una solicitud, habrá varios tiempos de respuesta.<br>● Si la solicitud no se enruta correctamente al servidor backend, se muestra un guion (-) como valor nulo para este campo. | Datos de punto flotante | 0.008, "-, 0.008", "0.008, 0.005: 0.004", or "0.008:" |
| upstream_addr | Dirección IP y número de puerto del servidor backend. Puede haber varios valores separados por comas y espacios, y cada valor tiene el formato de *IP address*}:{*Port number* o -.<br>Este parámetro solo está disponible para balanceadores de carga dedicados. | Dirección IP y número de puerto | -, or 192.168.1.2:8080 |

| Parámetro | Descripción | Descripción | Valor de ejemplo |
|---|---|---|---|
| http_user_agent | **http_user_agent** en la cabecera de solicitud recibida por el balanceador de carga, indicando el modelo del sistema y la información del navegador del cliente | Registra la información relacionada con el navegador. | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 |
| http_referer | **http_referer** en el encabezado de solicitud recibido por el balanceador de carga, indicando el enlace de página de la solicitud | Solicitar un enlace de página | http://10.154.197.90/ |
| http_x_forwarded_for | **http_x_forwarded_for** en la cabecera de solicitud recibida por el balanceador de carga, indicando la dirección IP del servidor proxy por el que pasa la solicitud | Dirección IP | 10.154.197.90 |
| lb_name | Nombre del balanceador de carga en el formato del **loadbalancer_***Load balancer ID* | String | loadbalancer_789424af-3fd2-4292-8c62-2a2dd7005175 |
| listener_name | Nombre del oyente en el formato de **listener_***Listener ID* | String | listener_fde03b66-f960-440e-954a-0be8b2b75093 |
| listener_id | ID de oyente (Este campo se puede ignorar) | String | - |
| pool_name | Nombre de grupo de servidor backend en el formato de **pool_***backend server group ID* | String | pool_066a5dc5-a3e4-4ea1-99f1-2a5716b681f6 |
| member_name | Nombre del servidor backend en el formato de **member_***server ID* (este campo aún no se admite). Puede haber varios valores separados por comas y espacios, y cada valor es un ID de miembro (**member_id**) o **-**. | String | member_47b07465-075a-4d2f-8ce9-0b9f39bff160 (Puede haber varios valores separados por comas y espacios, y cada valor es un ID de miembro (**member_id**) o **-**.) |
| tenant_id | ID del tenant | String | 04dd36f921000fe20f95c00bba986340 |

| Parámetro | Descripción | Descripción | Valor de ejemplo |
|---|---|---|---|
| eip_address:eip_port | EIP del balanceador de carga y del puerto frontend que se configuraron cuando se agregó el oyente | EIP del balanceador de carga y del puerto frontend que se configuraron cuando se agregó el oyente | 4.17.12.248:443 |
| upstream_addr_priv | Dirección IP y número de puerto del servidor backend. Puede haber varios valores separados por comas y espacios, y cada valor tiene el formato de *IP address*}:{*Port number* o -.<br>Este parámetro solo está disponible para balanceadores de carga dedicados. | Dirección IP y número de puerto | -, 192.168.1.2:8080 (Puede haber varios valores por comas y espacios, y cada valor tiene el formato de *IP address*}:{*Port number* o -.) |
| certificate_id | [HTTPS listener] ID de certificado utilizado para establecer una conexión SSL<br>Este campo aún no se admite. | String | 17b03b19-b2cc-454e-921b-4d187cce31dc |
| ssl_protocol | [HTTPS listener] Protocolo utilizado para establecer una conexión SSL<br>Para un oyente que no sea HTTPS, se muestra un guion (-) como valor nulo para este campo. | String | TLS 1.2 |
| ssl_cipher | [HTTPS listener] Suite de cifrado utilizada para establecer una conexión SSL<br>Para un oyente que no sea HTTPS, se muestra un guion (-) como valor nulo para este campo. | String | ECDHE-RSA-AES256-GCM-SHA384 |

| Parámetro | Descripción | Descripción | Valor de ejemplo |
| --- | --- | --- | --- |
| sni_domain_name | [HTTPS listener] Nombre de dominio SNI proporcionado por el cliente durante el protocolo de enlace SSL<br>Para un oyente que no sea HTTPS, se muestra un guion (-) como valor nulo para este campo. | String | www.test.com |
| tcpinfo_rtt | Tiempo de ida y vuelta (RTT) TCP entre el balanceador de carga y el cliente en microsegundos | Integer | 39032 |
| self_defined_header | Este campo está reservado. El valor predeterminado es -. | String | - |

## Ejemplo de log

```
1644819836.370 eb11c5a9-93a7-4c48-80fc-03f61f638595 [2022-02-14T14:23:56+08:00]
elb_01 192.168.1.1:888 200 "POST https://www.test.com/example/HTTP/1.1" 1411 251
3 0.011 "200" "0.000" "0.011" "0.011" "100.64.0.129:8080" "okhttp/3.13.1" "-" "-"
loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687 listener_20679192-8888-4e62-
a814-a2f870f62148 3333fd44fe3b42cbaa1dc2c641994d90 pool_89547549-6666-446e-9dbc-
e3a551034c46 "-" f2bc165ad9b4483a9b17762da851bbbb 121.64.212.1:443
"10.1.1.2:8080" - TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384 www.test.com 56704 -
```

En la siguiente tabla se describen los campos del log.

**Tabla 10-2** Campos en el log

| Campo | Valor de ejemplo |
| --- | --- |
| msec | 1644819836.370 |
| access_log_topic_id | eb11c5a9-93a7-4c48-80fc-03f61f638595 |
| time_iso8601 | [2022-02-14T14:23:56+08:00] |
| log_ver | elb_01 |
| remote_addr: remote_port | 192.168.1.1:888 |
| status | 200 |
| request_method scheme://host request_uri server_protocol | "POST https://www.test.com/example/1 HTTP/1.1" |
| request_length | 1411 |
| bytes_sent | 251 |

| Campo | Valor de ejemplo |
| --- | --- |
| body_bytes_sent | 3 |
| request_time | 0.011 |
| upstream_status | "200" |
| upstream_connect_time | "0.000" |
| upstream_header_time | "0.011" |
| upstream_response_time | "0.011" |
| upstream_addr | "100.64.0.129:8080" |
| http_user_agent | "okhttp/3.13.1" |
| http_referer | "-" |
| http_x_forwarded_for | "-" |
| lb_name | loadbalancer_295a7eee-9999-46ed-9fad-32a62ff0a687 |
| listener_name | listener_20679192-8888-4e62-a814-a2f870f62148 |
| listener_id | 3333fd44fe3b42cbaa1dc2c641994d90 |
| pool_name | pool_89547549-6666-446e-9dbc-e3a551034c46 |
| member_name | "-" |
| tenant_id | f2bc165ad9b4483a9b17762da851bbbb |
| eip_address:eip_port | 121.64.212.1:443 |
| upstream_addr_priv | "10.1.1.2:8080" |
| certificate_id | - |
| ssl_protocol | TLSv1.2 |
| ssl_cipher | ECDHE-RSA-AES256-GCM-SHA384 |
| sni_domain_name | www.test.com |
| tcpinfo_rtt | 56704 |
| self_defined_header | - |

Análisis de logs:

A las 14:23:56 GMT+08:00 del 14 de febrero de 2022, el balanceador de carga recibe una solicitud GET HTTP/1.1 de un cliente cuya dirección IP y número de puerto son 192.168.1.1 y 888, luego enruta la solicitud a un servidor backend cuya IP dirección y número de puerto

son 100.64.0.129 y 8080, y finalmente devuelve 200 OK al cliente después de recibir el código de estado del servidor backend.

Resultados del análisis:

El servidor backend responde a la solicitud normalmente.

## Configuración de la transferencia de log

Si desea analizar los registros de acceso más tarde, transfiera los registros a OBS o al Data Ingestion Service (DIS) para su almacenamiento.

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. Haga clic en  en la esquina superior izquierda y haga **Management & Governance** > **Log Tank Service**.
4. En el panel de navegación de la izquierda, elija **Log Transfer**.
5. En la página **Log Transfer**, haga clic en **Configure Log Transfer** en la esquina superior derecha.

1. Configure los parámetros. Para obtener más información, consulte la **Guía del usuario de Log Tank Service**.

# 11 Protección para las operaciones de misión críticas

## Escenarios

ELB admite una protección de operación sensible. Cuando realiza operaciones confidenciales en la consola de gestión, debe introducir una credencial que pueda probar su identidad. Solo puede realizar las operaciones correspondientes después de autenticar su identidad. Se recomienda activar la protección de operaciones para proteger su cuenta.

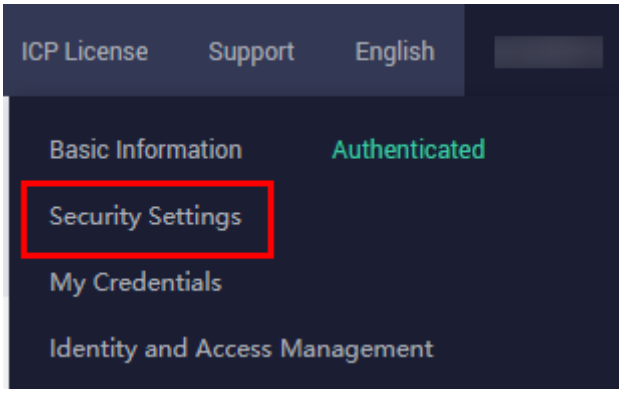
Esta función solo puede ser configurada por el administrador y tiene efecto para los recursos de su cuenta y los recursos de los usuarios de su cuenta. Los usuarios comunes solo tienen los permisos de vista. Para modificar los permisos, póngase en contacto con el administrador.

## Habilitación de la protección de la operación

La protección de la operación está deshabilitada de forma predeterminada. Realice las siguientes operaciones para habilitarlo:

1. Inicie sesión en la consola de gestión.
2. Mueva el cursor al nombre de usuario en la esquina superior derecha de la página y seleccione **Security Settings** en la lista desplegable.

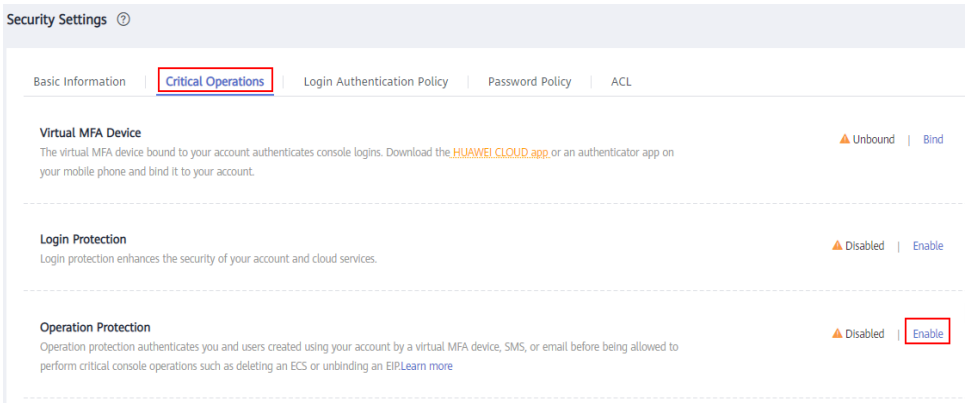
**Figura 11-1** Ajustes de seguridad




3. En la página **Security Settings**, elija **Critical Operations** > **Operation Protection** > **Enable**.

**Figura 11-2** Operaciones críticas




4. En la página **Operation Protection**, seleccione **Enable** para habilitar la protección de operación.

   Cuando usted o los usuarios de IAM de su cuenta realizan las operaciones críticas, por ejemplo, la eliminación de recursos de ECS, es necesario que introduzca un código de verificación basado en el método de verificación seleccionado.

   NOTA

   - Al realizar una operación crítica, se le pedirá que elija un método de verificación de correo electrónico, SMS y dispositivo MFA virtual.
     - Si solo ha vinculado un número de teléfono móvil, solo está disponible la verificación por SMS.
     - Si solo ha vinculado una dirección de correo electrónico, solo está disponible la verificación por correo electrónico.
     - Si no ha vinculado una dirección de correo electrónico, número de teléfono móvil o dispositivo MFA virtual, debe vincular uno para continuar con la operación crítica.
   - Puede cambiar el número de teléfono móvil, la dirección de correo electrónico y el dispositivo MFA virtual en la página **Información básica**.

## Verificación de la protección de la operación

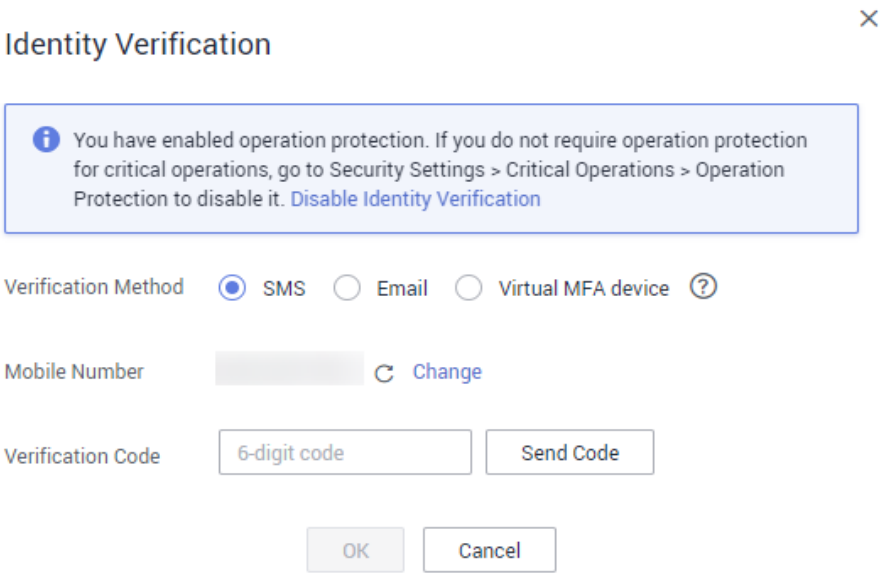
Una vez activada la protección de la operación, cuando realice una operación de misión crítica, el sistema verificará su identidad.

- Si ha vinculado una dirección de correo electrónico, introduzca el código de verificación de correo electrónico.
- Si ha vinculado un número de teléfono móvil, introduzca el código de verificación SMS.
- Si ha enlazado un dispositivo MFA virtual, introduzca un código de verificación dinámico de 6 dígitos del dispositivo MFA.

Cuando intenta eliminar un balanceador de carga, se muestra el siguiente cuadro de diálogo y debe seleccionar un método de verificación:

**Figura 11-3** Verificación de identidad

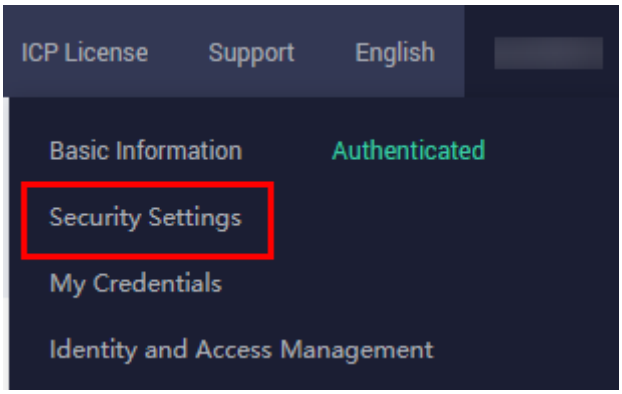



## Desactivación de la protección de operación

Realice las siguientes operaciones para deshabilitar la protección de la operación.

1. Inicie sesión en la consola de gestión.
2. Mueva el cursor al nombre de usuario en la esquina superior derecha de la página y seleccione **Security Settings** en la lista desplegable.

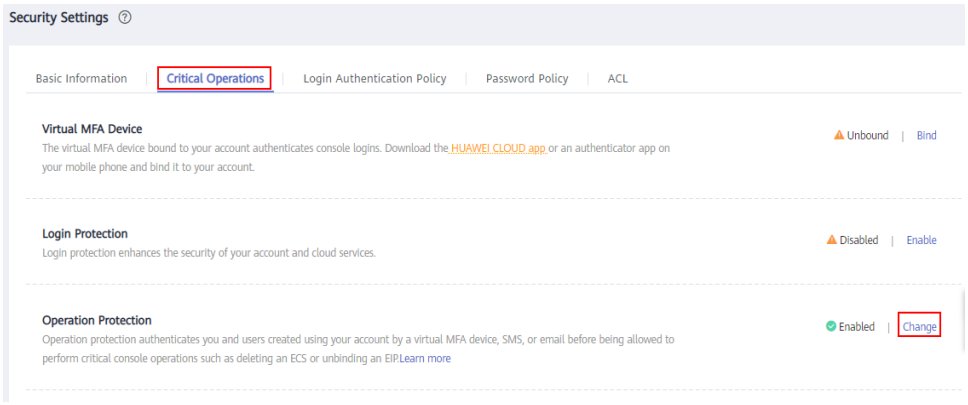
   **Figura 11-4** Ajustes de seguridad

3. En la página **Security Settings**, elija **Critical Operations** > **Operation Protection** > **Change**.

**Figura 11-5** Modificación de la configuración de protección de operación




4. En la página **Operation Protection**, seleccione **Disable** y haga clic en **OK**.

## Referencias

- **¿Cómo puedo vincular un dispositivo de MFA virtual?**
- **¿Cómo obtengo un código de verificación de MFA?**

# 12 Monitoreo

## 12.1 Métricas de monitoreo

### Descripción general

En esta sección se describe el espacio de nombres, las métricas que puede supervisar Cloud Eye y las dimensiones de estas métricas. Puede ver las métricas reportadas por ELB y las alarmas generadas en la consola de Cloud Eye. Para obtener más información, véase **Consulta de Métricas**.

### Espacio de nombres

SYS.ELB

## Métricas

**Tabla 12-1** Métricas soportadas por ELB

| ID de métrica | Nombre de usuario | Descripción | El valor | Objeto supervisado | Período de supervisión (datos brutos) |
|---|---|---|---|---|---|
| m1_cps | Concurrent Connections | Equilibrio de carga en la capa 4: número total de conexiones TCP y UDP desde el objeto supervisado a los servidores backend<br>Equilibrio de carga en la capa 7: número total de conexiones TCP de los clientes al objeto supervisado<br>Unidad: N/A | ≥ 0 | • Balanceador de carga dedicado<br>• Balanceador de carga Compartido<br>• Balanceador de carga dedicado - oyente<br>• Balanceador de carga Compartido - oyente | 1 minuto |
| m2_act_conn | Active Connections | Número de conexiones TCP y UDP en el estado **ESTABLISHED** entre el objeto supervisado y los servidores backend<br>Puede ejecutar el siguiente comando para ver las conexiones (servidores Windows y Linux): `netstat -an`<br>Unidad: N/A | ≥ 0 | | |
| m3_inact_conn | Inactive Connections | Número de conexiones TCP entre el objeto supervisado y los servidores backend excepto aquellos en el estado **ESTABLISHED**<br>Puede ejecutar el siguiente comando para ver las conexiones (servidores Windows y Linux): `netstat -an`<br>Unidad: N/A | ≥ 0 | | |

| ID de métrica | Nombre de usuario | Descripción | El valor | Objeto supervisado | Período de supervisión (datos brutos) |
|---|---|---|---|---|---|
| m4_ncps | New Connections | Número de conexiones TCP y UDP establecidas entre los clientes y el objeto supervisado por segundo<br>Unidad: vez/s | ≥ 0/ second | | |
| m5_in_pps | Incoming Packets | Número de paquetes recibidos por el objeto monitorizado por segundo<br>Unidad: paquete/s | ≥ 0/ second | | |
| m6_out_pps | Outgoing Packets | Número de paquetes enviados desde el objeto supervisado por segundo<br>Unidad: paquete/s | ≥ 0/ second | | |
| m7_in_Bps | Inbound Rate | Tráfico utilizado para acceder al objeto monitorizado desde Internet por segundo<br>Unidad: byte/s | ≥ 0 bytes/s | | |
| m8_out_Bps | Outbound Rate | Tráfico utilizado por el objeto monitorizado para acceder a Internet por segundo<br>Unidad: byte/s | ≥ 0 bytes/s | | |
| m9_abnormal_servers | Unhealthy Servers | Número de servidores back-end no saludables asociados con el objeto supervisado<br>Unidad: N/A | ≥ 0 | • Balanceador de carga dedicado<br>• Balanceador de carga Compartido | 1 minute |
| ma_normal_servers | Healthy Servers | Número de servidores backend en buen estado asociados con el objeto supervisado<br>Unidad: N/A | ≥ 0 | | |

| ID de métrica | Nombre de usuario | Descripción | El valor | Objeto supervisado | Período de supervisión (datos brutos) |
|---|---|---|---|---|---|
| m1e_server_rps | Reset Packets from Backend Servers | (TCP oyente métricas) Número de paquetes de reinicio reenviados por el objeto supervisado desde los servidores back-end a los clientes<br>Unidad: paquete/s | ≥ 0/ second | • Balanceador de carga Compartido<br>• Balanceador de carga Compartido - oyente | 1 minuto |
| m21_client_rps | Reset Packets from Clients | (TCP oyente métricas) Número de paquetes de reinicio reenviados por el objeto supervisado desde los clientes a los servidores backend<br>Unidad: paquete/s | ≥ 0/ second | | |
| m1f_lvs_rps | Reset Packets from Load Balancers | (TCP oyente métricas) Número de paquetes de reinicio generados por el objeto monitorizado por segundo<br>Unidad: paquete/s | ≥ 0/ second | | |
| m22_in_bandwidth | Inbound Bandwidth | Ancho de banda utilizado para acceder al objeto monitoreado desde Internet<br>Unidad: bit/s | ≥ 0 bit/s | | |
| m23_out_bandwidth | Outbound Bandwidth | Ancho de banda utilizado por el objeto monitorizado para acceder a Internet<br>Unidad: bit/s | ≥ 0 bit/s | | |

| ID de métrica | Nombre de usuario | Descripción | El valor | Objeto supervisado | Período de supervisión (datos brutos) |
|---|---|---|---|---|---|
| mb_l7_qps | Layer-7 Query Rate | Número de solicitudes que recibe el objeto supervisado por segundo<br>Unidad: Consulta/s | ≥ 0 query/s | • Balanceador de carga dedicado<br>• Balanceador de carga Compartido<br>• Balanceador de carga dedicado - oyente<br>• Balanceador de carga Compartido - oyente | 1 minuto |
| md_l7_http_3xx | 3xx Status Codes | Número de códigos de estado 3xx devueltos por el objeto monitorizado<br>Unidad: vez/s | ≥ 0/ second | • Balanceador de carga dedicado<br>• Balanceador de carga Compartido<br>• Balanceador de carga dedicado - oyente<br>• Balanceador de carga Compartido - oyente | 1 minuto |

| ID de métrica | Nombre de usuario | Descripción | El valor | Objeto supervisado | Período de supervisión (datos brutos) |
|---|---|---|---|---|---|
| mc_l7_http_2xx | 2xx Status Codes | Número de códigos de estado 2xx devueltos por el objeto monitorizado<br>Unidad: vez/s | ≥ 0/ second | • Balanceador de carga dedicado<br>• Balanceador de carga Compartido<br>• Balanceador de carga dedicado - oyente<br>• Balanceador de carga Compartido - oyente | 1 minuto |
| me_l7_http_4xx | 4xx Status Codes | Número de códigos de estado 4xx devueltos por el objeto monitorizado<br>Unidad: vez/s | ≥ 0/ second | | |
| mf_l7_http_5xx | 5xx Status Codes | Número de códigos de estado 5xx devueltos por el objeto monitorizado<br>Unidad: vez/s | ≥ 0/ second | | |
| m10_l7_http_other_status | Other Status Codes | Número de códigos de estado devueltos por el objeto supervisado, excepto los códigos de estado 2xx, 3xx, 4xx y 5xx<br>Unidad: vez/s | ≥ 0/ second | | |
| m11_l7_http_404 | 404 Not Found | Número de códigos de estado 404 No encontrado devueltos por el objeto monitorizado<br>Unidad: vez/s | ≥ 0/ second | | |
| m12_l7_http_499 | 499 Client Closed Request | Número de 499 códigos de estado de solicitud de cliente cerrado devueltos por el objeto supervisado<br>Unidad: vez/s | ≥ 0/ second | | |
| m13_l7_http_502 | 502 Bad Gateway | Número de 502 códigos de estado de Bad Gateway devueltos por el objeto supervisado<br>Unidad: vez/s | ≥ 0/ second | | |

| ID de métrica | Nombre de usuario | Descripción | El valor | Objeto supervisado | Período de supervisión (datos brutos) |
|---|---|---|---|---|---|
| m14_l7_rt | Average Layer-7 Response Time | Tiempo medio de respuesta del objeto monitorizado<br>El tiempo de respuesta comienza cuando el objeto supervisado recibe solicitudes de los clientes y finaliza cuando devuelve todas las respuestas a los clientes.<br>Unidad: ms | ≥ 0 ms | | |

### Dimensiones

| Clave | Valor |
|---|---|
| lbaas_instance_id | ● ID of a dedicated load balancer<br>● ID of un compartido load balancer |
| lbaas_listener_id | ● ID of a listener added to a dedicated load balancer<br>● ID of a listener added to un compartido load balancer |
| lbaas_pool_id | Backend server group ID |

# 12.2 Configuración de una regla de alarmas

Puede agregar, modificar y eliminar reglas de alarma. Para obtener más información, consulte la **Guía del usuario de Cloud Eye**.

## 12.2.1 Creación de una regla de alarma

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.

3. Haga clic en en la esquina superior izquierda y elija **Management & Governance** > **Cloud Eye**.
4. En el menú de la izquierda, seleccione **Alarm Management** > **Alarm Rules**.
5. En la página **Alarm Rules** mostrada, haga clic en **Create Alarm Rule**.

   Tabla 12-2 describe cómo crear una regla de alarma.

   **Tabla 12-2** Configuración de parámetros

| Parámetro | Configuración |
| --- | --- |
| Resource Type | Seleccione **Elastic Load Balance**. |
| Dimension | Seleccione cualquiera de las siguientes opciones:<br>● Balanceadores de carga elásticos<br>● Oyentes<br>● Grupo de servidores backend<br>**NOTA**<br>Para un balanceador de carga compartido, no se puede seleccionar **Listeners** como dimensión. |
| Other Parameters | Configure este parámetro según sea necesario. |

   Una vez creada la regla de alarma y activada la función de notificación, el sistema le envía automáticamente una notificación cuando se genera una alarma.

   NOTA

   Para obtener más información sobre las reglas de alarma de los balanceadores de carga y oyentes, consulte la **Guía del usuario de Cloud Eye**.

## 12.2.2 Modificación de una regla de alarma

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Haga clic en en la esquina superior izquierda y elija **Management & Governance** > **Cloud Eye**.
4. En el menú de la izquierda, seleccione **Alarm Management** > **Alarm Rules**.
5. En la página **Alarm Rules**, busque la regla de alarma y haga clic en **Modify** en la columna **Operation**.
   a. En la página **Modify Alarm Rule**, modifique los parámetros.
   b. Defina otros parámetros según sea necesario y, a continuación, haga clic en **Modify**.

      Una vez configurada la regla de alarma y activada la función de notificación, el sistema le envía automáticamente una notificación cuando se genera una alarma.

NOTA

Para obtener más información sobre las reglas de alarma de los balanceadores de carga y oyentes, consulte la **Guía del usuario de Cloud Eye**.

# 12.3 Consulta de Métricas

## Escenarios

Cloud Eye proporcionado por la plataforma de la nube pública monitorea los estados de ejecución de los balanceadores de carga.

Puede ver las métricas de cada balanceador de carga en la consola de ELB o en la consola de Cloud Eye.

La transmisión de datos de monitorización tarda un tiempo, por lo que el estado de cada balanceador de carga que se muestra en el panel de control de Cloud Eye no es su estado en tiempo real. Para un balanceador de carga recién creado o un oyente recién agregado, debe esperar entre 5 minutos y 10 minutos antes de poder ver sus métricas.

## Requisitos previos

- El balanceador de carga funciona correctamente.

  Si los servidores backend se detienen, fallan o se eliminan, no se muestran datos de supervisión.

  NOTA

  Cloud Eye deja de supervisar un balanceador de carga y lo elimina de la lista de objetos supervisados si sus servidores backend se han eliminado o están en estado detenido o defectuoso durante más de 24 horas. Sin embargo, las reglas de alarma configuradas no se eliminarán automáticamente.

- Ha interconectado ELB con Cloud Eye y configurado una regla de alarma para el balanceador de carga en la consola de Cloud Eye.

  Sin reglas de alarma, no hay datos de monitoreo. Para obtener más información, véase Configuración de una regla de alarmas.

- Si un usuario de IAM desea ver los datos de supervisión de ELB en la consola de Cloud Eye, se debe conceder al usuario de IAM el permiso de **ELB Administrator**. De lo contrario, el usuario de IAM no puede ver todos los datos de supervisión.

## Consulta de métricas de supervisión en la consola de ELB

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
4. Busque el balanceador de carga y haga clic en su nombre.
5. Vea las métricas de cada balanceador de carga y oyente.

a. Balanceador de carga: Haga clic en la ficha **Monitoring** y seleccione **Load balancer** para **Dimension**.

b. Oyente (de dos maneras):

   i. Haga clic en la ficha **Monitoring**, seleccione **Load oyente** para **Dimension** y busque el oyente de destino y vea las métricas de monitoreo.

   ii. Haga clic en el nombre del oyente de destino, cambie a la ficha **Monitoring** y vea las métricas de supervisión.

## Consulta de métricas de supervisión en la consola de Cloud Eye

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. Haga clic en en la esquina superior izquierda y elija **Management & Governance** > **Cloud Eye**.
4. En el panel de navegación de la izquierda, elija **Cloud Service Monitoring** >**Elastic Load Balance**.
5. En la página **Cloud Service Monitoring**, haga clic en el nombre del balanceador de carga. Como alternativa, busque el balanceador de carga y haga clic en **View Metric** en la columna **Operation**.
6. Seleccione el período de tiempo durante el que desea ver las métricas. Puede seleccionar un período de tiempo definido por el sistema (por ejemplo, la última hora) o especificar un período de tiempo.
7. Haga clic en **Select Metric** en la esquina superior derecha y seleccione las métricas que desea ver.

NOTA

Para obtener más información, consulte la Guía del usuario de Cloud Eye.

# 13 Auditoría

## 13.1 Operaciones de clave registradas por CTS

Puede usar CTS para registrar operaciones en ELB para consultas, auditorías y seguimiento.

Tabla 13-1 enumera las operaciones registradas por CTS.

**Tabla 13-1** Operaciones de ELB registradas por CTS

| Acción | Tipo de recurso | Trazado |
|---|---|---|
| Configuración de registros de acceso | logtank | createLogtank |
| Eliminación de registros de acceso | logtank | deleteLogtank |
| Creación de un certificado | certificate | createCertificate |
| Modificación de un certificado | certificate | updateCertificate |
| Supresión de un certificado | certificate | deleteCertificate |
| Creación de una comprobación de estado | healthmonitor | createHealthMonitor |
| Modificación de una comprobación de estado | healthmonitor | updateHealthMonitor |
| Eliminación de una comprobación de estado | healthmonitor | deleteHealthMonitor |
| Adición de una política de reenvío | l7policy | createL7policy |
| Modificación de una política de reenvío | l7policy | updateL7policy |

| Acción | Tipo de recurso | Trazado |
| --- | --- | --- |
| Eliminación de una política de reenvío | l7policy | deleteL7policy |
| Adición de una regla de reenvío | l7rule | createl7rule |
| Modificación de una regla de reenvío | l7rule | updateL7rule |
| Supresión de una regla de reenvío | l7rule | deleteL7rule |
| Adición de un oyente | listener | createListener |
| Modificación de un oyente | listener | updateListener |
| Eliminación de un oyente | listener | deleteListener |
| Creación de un balanceador de carga | loadbalancer | createLoadbalancer |
| Modificación de un balanceador de carga | loadbalancer | updateLoadbalancer |
| Eliminación de un balanceador de carga | loadbalancer | deleteLoadbalancer |
| Adición de un servidor backend | member | createMember |
| Modificación de un servidor backend | member | updateMember |
| Extracción de un servidor backend | member | batchUpdateMember |
| Creación de un grupo de servidores backend | pool | createPool |
| Modificación de un grupo de servidores backend | pool | updatPool |
| Eliminación de un grupo de servidores backend | pool | deletePool |

# 13.2 Consulta de trazas

## Escenarios

CTS registra las operaciones realizadas en ELB y le permite ver los registros de operaciones de los últimos siete días en la consola CTS. Para consultar estos registros, realice las siguientes operaciones.

## Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
3. En **Management & Governance**, haga clic en **Cloud Trace Service**.
4. En el panel de navegación de la izquierda, elija **Trace List**.
5. Especifique los filtros utilizados para consultar seguimientos. Los siguientes filtros están disponibles:
   - **Trace Type**, **Trace Source**, **Resource Type**, y **Search By**

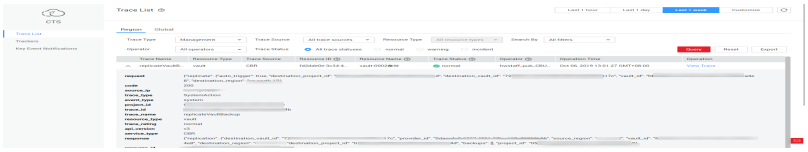
     Seleccione un filtro de la lista desplegable.

     Si selecciona **Trace name** para **Search By** también debe seleccionar un nombre de seguimiento específico.

     Si selecciona **Resource ID** para **Search By**, seleccione o introduzca un ID de recurso específico.

     Si selecciona **Resource name** para **Search By**, seleccione o introduzca un nombre de recurso específico.
   - **Operator**: Seleccione un operador específico (en el nivel de usuario en lugar de en el nivel de tenant).
   - **Trace Status**: las opciones disponibles incluyen **All trace statuses**, **Normal**, **Warning**, e **Incident**. Solo se puede habilitar una de ellas.
   - Intervalo de tiempo: Puede consultar las trazas generadas en cualquier intervalo de tiempo de los últimos siete días.
6. Haga clic en a la izquierda de la traza requerida para ampliar sus detalles.

**Figura 13-1** Ampliación de los detalles de seguimiento



7. Haga clic en **View Trace** en la columna **Operation** para ver los detalles del seguimiento.

**Figura 13-2** Ver traza


```
"context": {
    "code": "204",
    "source_ip": "10.45.152.59",
    "trace_type": "ApiCall",
    "event_type": "system",
    "project_id": "0503dda897000fed2f78c00909158a4d",
    "trace_id": "116a2aff-deb8-11e9-95f5-d5c0b02a9b97",
    "trace_name": "deleteMember",
    "resource_type": "member",
    "trace_rating": "normal",
    "api_version": "v2.0",
    "service_type": "ELB",
    "response": "{\"member\": {\"project_id\": \"0503dda897000fed2f78c00909158a4d\", \"name\": \"9646e73b-338c-
    "resource_id": "                                    ,
    "tracker_name": "system",
    "time": "1569321775225",
    "resource_name": "9646e73b-338c-4d27-a17c-219be532812c",
    "record_time": "1569321775903",
    "user": {
        "domain": {
            "name": "
            "id": "0503dda878000fed0f75c0096d70a960"
        },
```

Para obtener detalles sobre los campos clave en el seguimiento, consulte la **Guía del usuario de Cloud Trace Service**.

## Ejemplo de trazas

- Creación de un balanceador de carga

```
request {"loadbalancer":{"name":"elb-test-
zcy","description":"","tenant_id":"05041fffa40025702f6dc009cc6f8f33","vip_subn
et_id":"ed04fd93-e74b-4794-b63e-e72baa02a2da","admin_state_up":true}}
code 201
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id b39b21a1-8d49-11ec-b548-2be046112888
trace_name createLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"description": "", "provisioning_status":
"ACTIVE", "provider": "vlb", "project_id":
"05041fffa40025702f6dc009cc6f8f33", "vip_address": "172.18.0.205", "pools":
[], "operating_status": "ONLINE", "name": "elb-test-zcy", "created_at":
"2022-02-14T03:53:39", "listeners": [], "id": "7ebe23cd-1d46-4a49-
b707-1441c7f0d0d1", "vip_port_id": "5b36ff96-3773-4736-83cf-38c54abedeea",
"updated_at": "2022-02-14T03:53:41", "tags": [], "admin_state_up": true,
"vip_subnet_id": "ed04fd93-e74b-4794-b63e-e72baa02a2da", "tenant_id":
"05041fffa40025702f6dc009cc6f8f33"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:53:42 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:53:42 GMT+08:00
request_id
user {"domain": {"name": "CBUInfo", "id": "0503dda87802345ddafed096d70a960"},
"name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}
```

- Eliminación de un balanceador de carga

```
request
code 204
source_ip 124.71.93.36
trace_type ConsoleAction
event_type system
project_id 05041fffa40025702f6dc009cc6f8f33
trace_id 4f838bbf-8d4a-11ec-a1fe-1f93fdaf3bec
trace_name deleteLoadbalancer
resource_type loadbalancer
trace_rating normal
api_version v2.0
service_type ELB
response {"loadbalancer": {"listeners": [], "vip_port_id":
"5b36ff96-3773-4736-83cf-38c54abedeea", "tags": [], "tenant_id":
"05041fffa40025702f6dc009cc6f8f33", "admin_state_up": true, "id":
"7ebe23cd-1d46-4a49-b707-1441c7f0d0d1", "operating_status": "ONLINE",
"description": "", "pools": [], "vip_subnet_id": "ed04fd93-e74b-4794-b63e-
e72baa02a2da", "project_id": "05041fffa40025702f6dc009cc6f8f33",
"provisioning_status": "ACTIVE", "name": "elb-test-zcy", "created_at":
"2022-02-14T03:53:39", "vip_address": "172.18.0.205", "updated_at":
"2022-02-14T03:53:41", "provider": "vlb"}}
resource_id 7ebe23cd-1d46-4a49-b707-1441c7f0d0d1
tracker_name system
time 2022/02/14 11:58:03 GMT+08:00
resource_name elb-test-zcy
record_time 2022/02/14 11:58:03 GMT+08:00
request_id
user {"domain": {"name": CBUInfo", "id": "0503dda87802345ddafed096d70a960"},
"name": "zcy", "id": "09f106afd2345cdeff5c009c58f5b4a"}
```

# 14 Cuotas

## ¿Qué es una cuota?

Las cuotas pueden limitar el número o la cantidad de recursos disponibles para los usuarios, como el número máximo de ECS o discos EVS que se pueden crear.

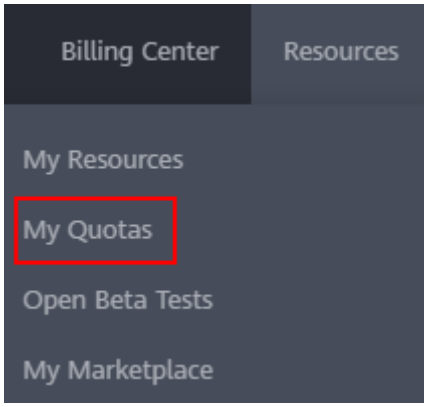
Si la cuota de recursos existente no puede cumplir con los requisitos de servicio, puede solicitar una cuota más alta.

## ¿Cómo puedo ver mis cuotas?

1. Inicie sesión en la consola de gestión.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la esquina superior derecha de la página, seleccione **Resources** > **My Quotas**.

   Se muestra la página **Service Quota**.

   **Figura 14-1** Mis cuotas

4. Vea la cuota usada y total de cada tipo de recursos en la página mostrada.

   Si una cuota no puede cumplir con los requisitos de servicio, solicite una cuota más alta.

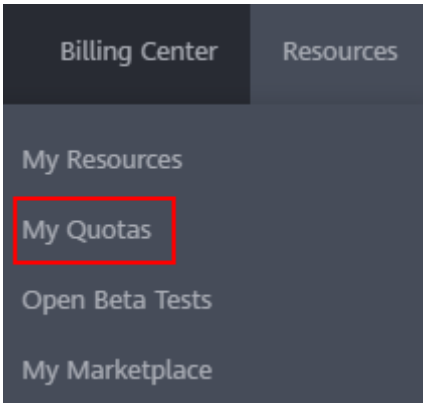
## ¿Cómo solicito una cuota más alta?

1. Inicie sesión en la consola de gestión.

2. En la esquina superior derecha de la página, seleccione **Resources** > **My Quotas**.
   Se muestra la página **Service Quota**.

   **Figura 14-2** Mis cuotas

3. Haga clic en **Increase Quota**.
4. En la página **Create Service Ticket**, configure los parámetros según sea necesario.
   En el área **Problem Description**, rellene el contenido y el motivo del ajuste.
5. Después de configurar todos los parámetros necesarios, seleccione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** y haga clic en **Submit**.

# 15 Apéndice

## 15.1 Configuración del módulo TOA

### Escenarios

ELB proporciona estrategias personalizadas para gestionar el acceso al servicio. Antes de que estas estrategias se puedan personalizar, se requieren las direcciones IP de los clientes contenidas en las solicitudes. Para obtener las direcciones IP, puede instalar el módulo del núcleo TCP Option Address (TOA) en servidores backend.

Esta sección proporciona operaciones detalladas para compilar el módulo en el SO si utiliza TCP para distribuir el tráfico entrante.

Las operaciones para los SO de Linux con la versión del kernel de 2.6.32 son diferentes de aquellas para los SO de Linux con la versión del kernel de 3.0 o posterior.

NOTA

- TOA no admite oyentes usando el protocolo UDP.
- El módulo puede funcionar correctamente en los siguientes SO y los métodos para instalar otras versiones del kernel son similares:
  - CentOS 6.8 (kernel version 2.6.32)
  - SUSE 11 SP3 (kernel version 3.0.76)
  - CentOS 7 and CentOS 7.2 (kernel version 3.10.0)
  - Ubuntu 16.04.3 (kernel version 4.4.0)
  - Ubuntu 18.04 (kernel version 4.15.0)
  - Ubuntu 20.04 (Kernel version 5.4.0)
  - OpenSUSE 42.2 (kernel version 4.4.36)
  - Debian 8.2.0 (kernel version 3.16.0)

### Requisitos previos

- El entorno de desarrollo para compilar el módulo debe ser el mismo que el del núcleo actual.
- Los servidores pueden acceder a los repositorios SO.

- Los usuarios que no sean root deben tener permisos sudo.

## Procedimiento

- En las siguientes operaciones, la versión del kernel de Linux es 3.0 o posterior.

1. Preparar el entorno de compilación.

   NOTA

   Durante la instalación, descargue el paquete de desarrollo del módulo requerido desde Internet si no se puede encontrar en el origen.

   Las siguientes son operaciones para compilar el módulo en diferentes SO de Linux. Realizar las operaciones adecuadas.

   – CentOS

     i. Ejecute el siguiente comando para instalar GCC:

     **sudo yum install gcc**

     ii. Ejecute el siguiente comando para instalar la herramienta make:

     **sudo yum install make**

     iii. Ejecute el siguiente comando para instalar el paquete de desarrollo de módulos (el encabezado del paquete y la biblioteca de módulos deben tener la misma versión que el núcleo):

     **sudo yum install kernel-devel-`uname -r`**

     NOTA

     Durante la instalación, descargue el paquete de desarrollo del módulo requerido desde la siguiente dirección si no se encuentra en el origen:

     https://mirror.netcologne.de/oracle-linux-repos/ol7_latest/getPackage/

     Por ejemplo, para instalar 3.10.0-693.11.1.el7.x86_64, ejecute el siguiente comando:

     **rpm -ivh kernel-devel-3.10.0-693.11.1.el7.x86_64.rpm**

   – Ubuntu y Debian

     i. Ejecute el siguiente comando para instalar GCC:

     **sudo apt-get install gcc**

     ii. Ejecute el siguiente comando para instalar la herramienta make:

     **sudo apt-get install make**

     iii. Ejecute el siguiente comando para instalar el paquete de desarrollo de módulos (el encabezado del paquete y la biblioteca de módulos deben tener la misma versión que el núcleo):

     **sudo apt-get install linux-headers-`uname -r`**

   – SUSE

     i. Ejecute el siguiente comando para instalar GCC:

     **sudo zypper install gcc**

     ii. Ejecute el siguiente comando para instalar la herramienta make:

     **sudo zypper install make**

     iii. Ejecute el siguiente comando para instalar el paquete de desarrollo de módulos (el encabezado del paquete y la biblioteca de módulos deben tener la misma versión que el núcleo):

**sudo zypper install kernel-default-devel**

2. Compilar el módulo.

   a. Utilice la herramienta git y ejecute el siguiente comando para descargar el código fuente del módulo:

   **git clone https://github.com/Huawei/TCP_option_address.git**

   NOTA

   Si la herramienta git no está instalada, descargue el código fuente del módulo desde el siguiente enlace:

   **https://github.com/Huawei/TCP_option_address**

   b. Ejecute los siguientes comandos para ingresar al directorio de código fuente y compilar el módulo:

   **cd src**

   **make**

   Si no se solicita ningún aviso o código de error, la compilación se ha realizado correctamente. Verifique que el archivo **toa.ko** se haya generado en el directorio actual.

   NOTA

   Si el mensaje de error, "config_retpoline=y but not supported by the compiler, Compiler update recommended" se muestra, la versión de GCC es demasiado antigua. Actualice el GCC a una versión posterior.

3. Cargue el módulo.

   a. Ejecute el siguiente comando para cargar el módulo:

   **sudo insmod toa.ko**

   b. Ejecute el siguiente comando para comprobar la carga del módulo y ver la información de salida del kernel:

   **dmesg | grep TOA**

   Si **TOA: toa loaded** se muestra en la salida del comando, el módulo se ha cargado.

   NOTA

   Después de compilar el módulo CoreOS en el contenedor, cópielo en el sistema host y cárguelo. El contenedor para compilar el módulo comparte el directorio **/lib/modules** con el sistema host, por lo que puede copiar el módulo en el contenedor a este directorio, permitiendo que el sistema host lo use.

4. Establezca el script para habilitarlo para cargar automáticamente el módulo.

   Para que el módulo entre en vigor cuando se inicie el sistema, agregue el comando para cargar el módulo a su script de inicio.

   Puede utilizar cualquiera de los siguientes métodos para cargar automáticamente el módulo:

   – Agregue el comando para cargar el módulo en un script de inicio personalizado según sea necesario.
   – Realice las siguientes operaciones para configurar un script de inicio:

     i. Cree el archivo **toa.modules** en el directorio **/etc/sysconfig/modules/**. Este archivo contiene el script de carga del módulo.

     A continuación se muestra un ejemplo del contenido del archivo **toa.modules**.

**#!/bin/sh**

**/sbin/modinfo -F filename /root/toa/toa.ko > /dev/null 2>&1**

**if [ $? -eq 0 ]; then**

**/sbin/insmod /root/toa/toa.ko**

**fi**

**/root/toa/toa.ko** es la ruta del archivo del módulo. Necesita reemplazarlo con su camino real.

ii. Ejecute el siguiente comando para agregar permisos de ejecución para el script de inicio **toa.modules**:

**sudo chmod +x /etc/sysconfig/modules/toa.modules**

NOTA

Si se actualiza el kernel, el módulo actual ya no coincidirá. Compilar el módulo de nuevo.

5. Instale el módulo en varios servidores.

   Para cargar el módulo en el mismo SO, copie el archivo **toa.ko** en los servidores donde se va a cargar el módulo y luego realice las operaciones en **3**.

   Una vez que el módulo se ha cargado correctamente, las aplicaciones pueden obtener la dirección IP real contenida en la solicitud.

   NOTA

   El SO del servidor debe tener la misma versión que el kernel.

6. Verifique el módulo.

   Después de que el módulo se haya instalado correctamente, la dirección de origen se puede obtener directamente. A continuación se proporciona un ejemplo de verificación.

   Ejecute el siguiente comando para iniciar un servicio HTTP simple en el servidor backend donde está instalado Python:

   **python -m SimpleHTTPServer** *port*

   El valor del **port** debe ser el mismo que el puerto configurado para el servidor backend, y el valor predeterminado es 80.

   Acceda a la dirección IP del balanceador de carga desde un cliente. Los registros de acceso en el servidor son los siguientes:

   ```
   192.168.0.90 - - [06/Aug/2020 14:24:21] "GET / HTTP/1.1" 200 -
   ```

   NOTA

   **192.168.0.90** indica la dirección IP de origen del cliente que obtiene el servidor backend.

- En las siguientes operaciones, la versión del kernel de Linux es 2.6.32.

  NOTA

  El complemento TOA soporta los sistemas operativos (imagen CentOS 6.8) con un núcleo de 2.6.32-xx. Realice los siguientes pasos para configurar el módulo:

1. Obtenga el paquete de código fuente del núcleo **Linux-2.6.32-220.23.1.el6.x86_64.rs.src.tar.gz** que contiene el módulo en el siguiente enlace:

   **http://kb.linuxvirtualserver.org/images/3/34/Linux-2.6.32-220.23.1.el6.x86_64.rs.src.tar.gz**

2. Descomprima el paquete de código fuente del núcleo.
3. Modifique parámetros de compilación.
   a. Abra la carpeta **linux-2.6.32-220.23.1.el6.x86_64.rs**.
   b. Edite el archivo **net/toa/toa.h**.
      Cambie el valor de **#define TCPOPT_TOA200** a **#define TCPOPT_TOA254**.
   c. En la página del shell, ejecute los siguientes comandos:
      **sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config**
      **echo -e '\n# toa\nCONFIG_TOA=m' >> .config**
      Después de la configuración, el módulo IPv6 se compila en el núcleo. TOA se compila en un módulo separado y se puede iniciar y detener independientemente.
   d. Edita **Makefile**.
      Puede añadir una descripción al final de **EXTRAVERSION =**. Esta descripción se mostrará en **uname -r**, por ejemplo, **-toa**.
4. Ejecute el siguiente comando para compilar el paquete de software:
   **make -j *n***

   NOTA

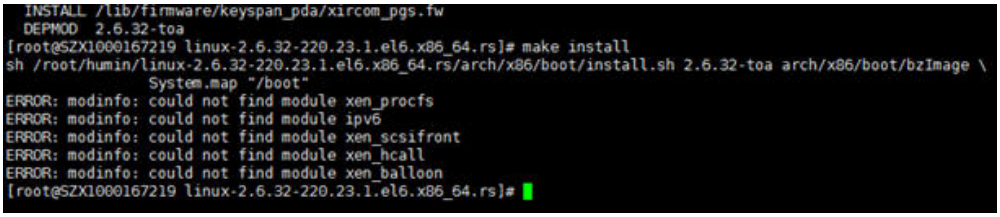
   *n* indica el número de vCPUs. Por ejemplo, si hay cuatro vCPU, *n* debe establecerse en 4.
5. Ejecute el siguiente comando para instalar el módulo:
   **make modules_install**
   La siguiente información aparecerá en la pantalla.

   **Figura 15-1** Instalación del módulo

   
   
6. Ejecute el siguiente comando para instalar el kernel:
   **make install**
   La siguiente información aparecerá en la pantalla.

**Figura 15-2** Instalación del kernel

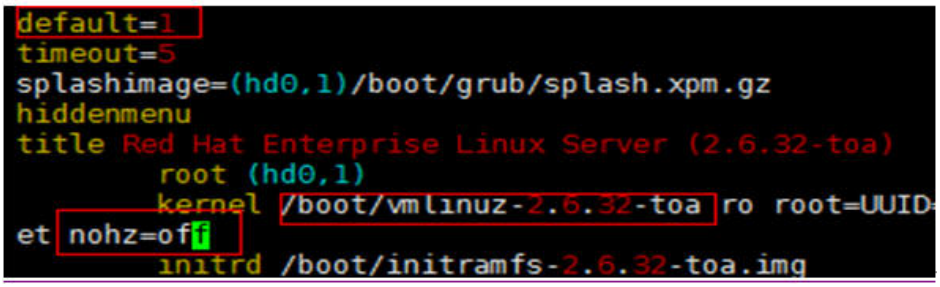



7. Abra el archivo **/boot/grub/grub.conf** y configure el núcleo para que se inicie cuando se inicie el sistema.

   a. Cambie el kernel de inicio predeterminado del primer kernel al kernel cero cambiando **default=1** a **default=0**.

   b. Agregue el parámetro **nohz=off** al final de la línea que contiene el kernel **vmlinuz-2.6.32-toa**. Si **nohz** no está deshabilitado, la utilización de CPU0 puede ser alta y sobrecargar el núcleo.

   **Figura 15-3** Archivo de configuración




   c. Guarde la modificación y salga. Reinicie el sistema operativo.

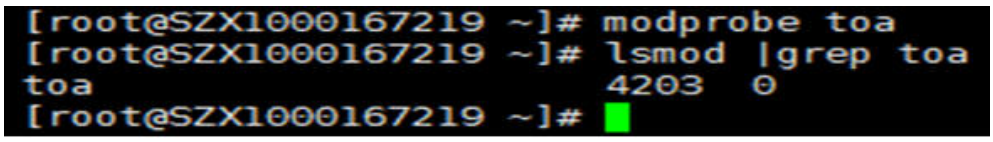
   Durante el reinicio, el sistema cargará el kernel vmlinuz-2.6.32-toa.

8. Después del reinicio, ejecute el siguiente comando para cargar el módulo:

   **modprobe toa**

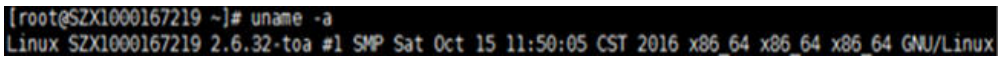
   Agregue el comando **modprobe toa** tanto al script de inicio como al script de monitoreo programado del sistema.

   **Figura 15-4** Agrega el comando **modprobe toa**




   Después de cargar el módulo, consulte la información del núcleo.

   **Figura 15-5** Consulta del kernel




9. Verifique el módulo.

   Después de que el módulo se haya instalado correctamente, la dirección de origen se puede obtener directamente. A continuación se proporciona un ejemplo de verificación.

Ejecute el siguiente comando para iniciar un servicio HTTP simple en el servidor backend donde está instalado Python:

**python -m SimpleHTTPServer** *port*

El valor del **port** debe ser el mismo que el puerto configurado para el servidor backend, y el valor predeterminado es 80.

Acceda a la dirección IP del balanceador de carga desde un cliente. Los registros de acceso en el servidor son los siguientes:

```
192.168.0.90 - - [06/Aug/2020 14:24:21] "GET / HTTP/1.1" 200 -
```

NOTA

**192.168.0.90** indica la dirección IP de origen del cliente que obtiene el servidor backend.