Elastic Load Balance

Preguntas frecuentes

Edición 03

Fecha 2022-11-01

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 Preguntas populares

2 Anormalidad del servicio

2.1 ¿Por qué no puedo acceder a mis servidores backend con un balanceador de carga?

Síntoma

Esta sección de preguntas frecuentes proporciona una guía para que pueda solucionar los siguientes problemas:

- No se puede acceder a los servidores backend con un balanceador de carga.
- Puede acceder al balanceador de carga desde una dirección IP privada, pero no desde una dirección IP pública.
- Los servidores backend se consideran no saludables.

Antecedentes

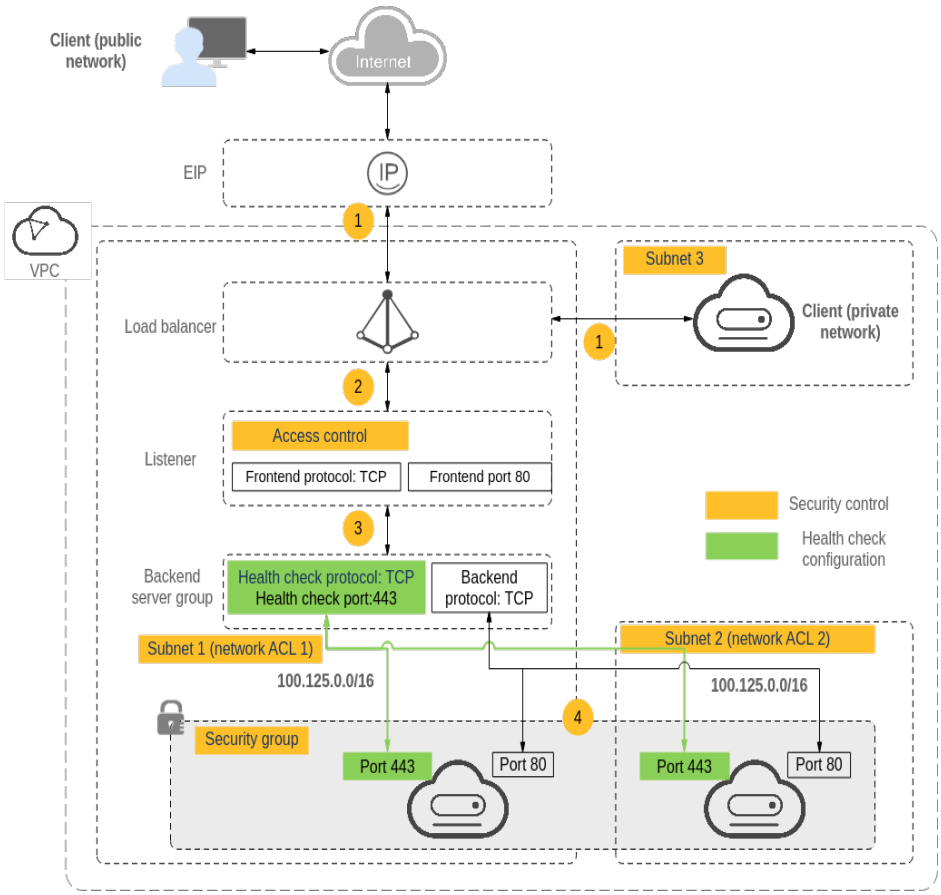
Figura 2-1 muestra cómo los clientes acceden a los servidores backend con un balanceador de carga.

1. El balanceador de carga de red pública utiliza una EIP para recibir tráfico por Internet, mientras que el balanceador de carga de red privada recibe tráfico desde dentro de la VPC.
2. El balanceador de carga recibe tráfico entrante utilizando el protocolo frontend y el puerto configurado para el oyente.
3. El oyente comprueba el estado de los servidores backend. Solo los servidores backend sanos pueden recibir tráfico del oyente.
4. El oyente reenvía el tráfico a los servidores backend según sus ponderaciones y las reglas de escucha.

En general, el problema se debe probablemente a un problema de control de acceso (las partes en amarillo) o a una configuración de comprobación de estado (las partes verdes).

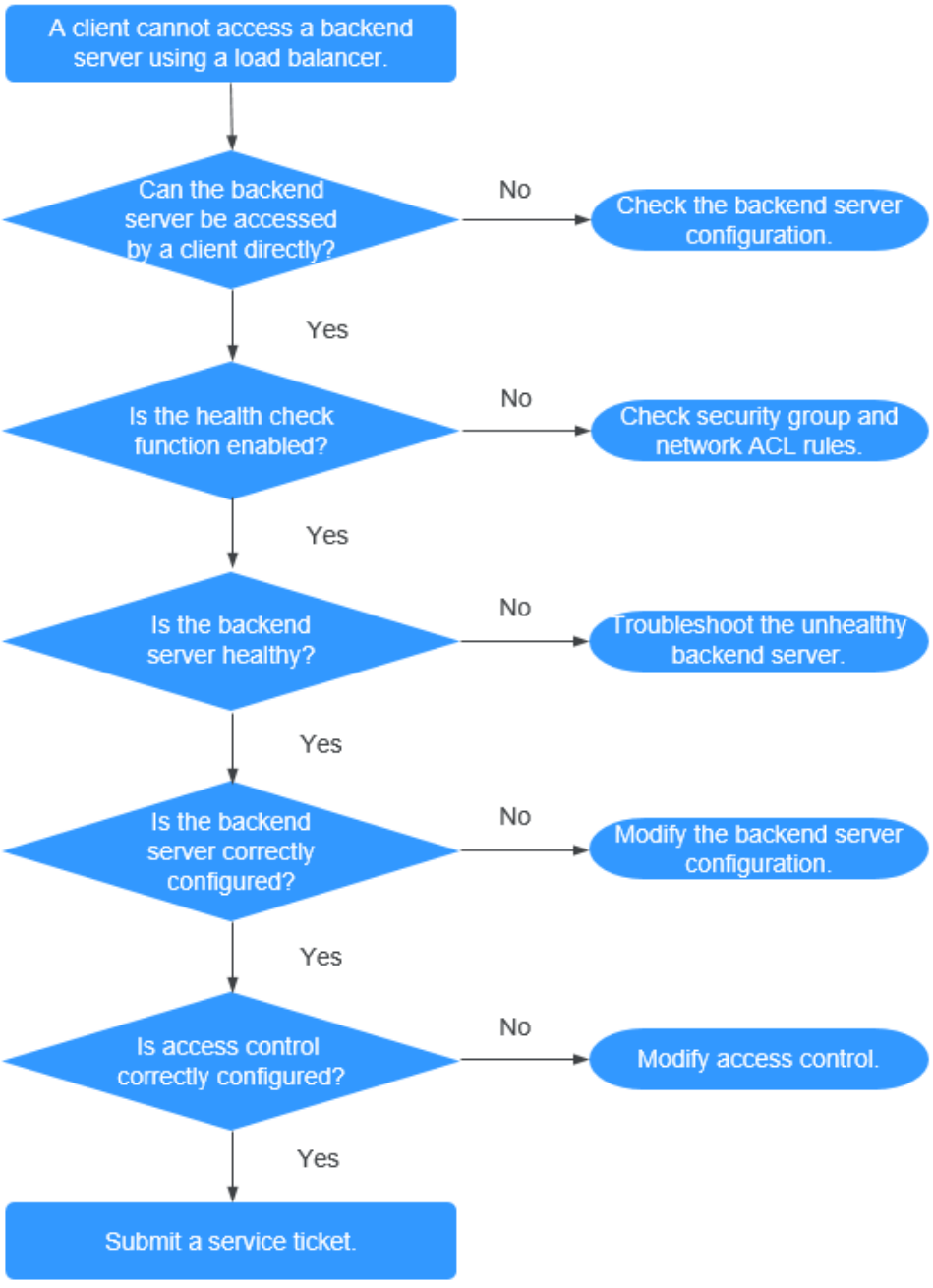
La solución de problemas debe comenzar con los servidores backend, luego pasar al balanceador de carga y, finalmente, a los clientes.

Figura 2-1 Cómo los clientes acceden a los servidores backend con un balanceador de carga



Proceso de solución de problemas

Figura 2-2 Proceso de solución de problemas



1. **Compruebe si se puede acceder directamente al servidor backend.** Utilice el cliente para acceder al servidor backend y verifique que la configuración del servidor backend y la configuración de la aplicación sean correctas.
2. **Compruebe si la comprobación de estado está habilitada en la consola.**
3. **Compruebe si el resultado de la comprobación de estado del servidor backend en la consola.** Si el servidor backend no está sano, el balanceador de carga no encaminará el tráfico hacia él.

4. **Compruebe si la ponderación y el puerto del servidor backend están configurados correctamente en la consola.**
5. **Compruebe si el control de acceso está habilitado y la dirección IP del cliente puede acceder al oyente en la consola.**

Paso 1: Comprobar si se puede acceder directamente al servidor backend

Utilice un cliente para acceder al servidor backend para determinar si el fallo es causado por el balanceador de carga o el servidor backend. Para ello, asegúrese de que las reglas de ACL de red permiten las comunicaciones entre el cliente y el servidor backend.

- Clientes en la red pública: Vincule una EIP al servidor backend. Una vez completada la verificación, libere la EIP.
- Clientes en la red privada: No se requiere la EIP. Si el cliente está en otra VPC, configure una interconexión de VPC.

Si el fallo persiste, vaya a **Paso 2: Comprobar si la comprobación de estado está habilitada**.

Paso 2: Comprobar si la comprobación de estado está habilitada

Si el cliente puede acceder directamente al servidor backend, compruebe si la comprobación de estado está habilitada. Si la comprobación de estado está habilitada pero el servidor backend se detecta mal, el balanceador de carga no encaminará el tráfico hacia él.

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 nombre del balanceador de carga.
5. En la página de ficha **Listeners**, compruebe si la comprobación de estado está habilitada.
   - Si la comprobación de estado está activada, vaya a **Paso 3: Comprobar si el servidor backend está sano**.
   - Si la comprobación de estado no está habilitada:
     - Balanceadores de carga Compartidoes: Compruebe si las reglas de grupo de seguridad de los servidores backend y las reglas de ACL de red permiten el tráfico de 100.125.0.0/16.
     - Balanceadores de carga dedicados: Compruebe si las reglas del grupo de seguridad backend permiten el acceso desde el bloque CIDR de VPC donde funciona la subred backend de ELB.

     Este bloque CIDR es utilizado por ELB para acceder a servidores backend y no tiene riesgos de seguridad. Si se permite el tráfico pero el fallo persiste, vaya a **Paso 4: Comprobar si la configuración del servidor backend es correcta**.

⚠ ATENCIÓN

- Balanceadores de carga compartidos: Si **Transfer Client IP Address** está habilitada para un oyente de TCP o de UDP, no es necesario configurar reglas de grupo de seguridad y reglas de ACL de red para permitir el tráfico de 100.125.0.0/16 y direcciones IP del cliente a los servidores backend.
- Balanceadores de carga dedicados: Si **IP as a Backend** no está habilitado para un balanceador de carga que tiene un oyente de TCP o de UDP, no hay necesidad de configurar reglas de grupo de seguridad y reglas de ACL de red para permitir el tráfico desde la subred backend donde el balanceador de carga se despliega en los servidores backend.

Paso 3: Comprobar si el servidor backend está sano

Si la comprobación de estado está habilitada pero el servidor backend se detecta mal, el balanceador de carga no encaminará el tráfico hacia él.

- Si el servidor backend no está sano, rectifique la falla consultando **¿Cómo soluciono problemas de un servidor backend insalubre?**
- Si el servidor de backend está en buen estado, vaya a **Paso 4: Comprobar si la configuración del servidor backend es correcta**.

Si el fallo persiste, vaya a **Paso 4: Comprobar si la configuración del servidor backend es correcta**.

Paso 4: Comprobar si la configuración del servidor backend es correcta

1. Elija **Backend Server Groups** > **Backend Servers** para ver los parámetros del servidor backend:
   - **Weight**: Si la ponderación se establece en 0, el tráfico no se reenviará al servidor.
   - **Backend port**: Debe ser el mismo que el puerto utilizado por el servidor backend.
2. En la página de ficha **Listeners**, localice el oyente de TCP o de UDP y compruebe si **Transfer Client IP Address** está habilitado.
   - Si esta función está habilitada, el balanceador de carga utiliza la dirección IP del cliente para acceder al servidor backend. En este caso, configure las reglas de grupo de seguridad y de ACL de red para permitir el acceso desde esta dirección IP.

     Además, si esta función está habilitada, no se puede usar un servidor como cliente y servidor backend. Esto se debe a que el servidor backend determina que el paquete es enviado por un host local basado en la dirección IP de origen y no devolverá el paquete de respuesta al balanceador de carga.
   - Si esta función está deshabilitada, verifique que el grupo de seguridad permita el tráfico desde el intervalo de direcciones IP correspondiente al servidor backend.
     - Balanceadores de carga dedicados: asegúrese de que el grupo de seguridad permita el tráfico desde la subred backend donde reside el balanceador de carga dedicado al servidor backend.
     - Balanceadores de carga compartidos: asegúrese de que el grupo de seguridad permita el tráfico desde 100.125.0.0/16 al servidor backend.

Si el fallo persiste, vaya a **Paso 5: Comprobar si el control de acceso está habilitado**.

Paso 5: Comprobar si el control de acceso está habilitado

En la pestaña **Summary** del oyente, compruebe si el control de acceso está habilitado y si el cliente puede acceder al oyente.

Enviar un ticket de servicio

Si el problema persiste, **envíe un ticket de servicio**.

2.2 ¿Qué puedo hacer si no se puede acceder a ELB o se interrumpe el enrutamiento de tráfico?

1. Compruebe el estado de los servidores backend. Si un servidor backend no está sano, el tráfico se enrutará a otros servidores sanos. Rectifique el fallo de la comprobación de estado y vuelva a acceder a ELB.
2. Compruebe si las reglas del grupo de seguridad permiten el acceso desde el intervalo de direcciones IP correspondiente.
   - Balanceadores de carga dedicados: Compruebe si el grupo de seguridad que contiene el servidor backend tiene reglas entrantes para permitir el tráfico desde la subred backend donde se despliega el balanceador de carga.
   - Balanceadores de carga compartidos: Compruebe si el grupo de seguridad que contiene el servidor backend tiene reglas entrantes para permitir el tráfico de 100.125.0.0/16.

   ⚠ ATENCIÓN

   - Balanceadores de carga compartidos: Si **Transfer Client IP Address** está habilitada para un oyente de TCP o de UDP, no es necesario configurar reglas de grupo de seguridad y reglas de ACL de red para permitir el tráfico de 100.125.0.0/16 y direcciones IP del cliente a los servidores backend.
   - Balanceadores de carga dedicados: Si **IP as a Backend** no está habilitado para un balanceador de carga que tiene un oyente de TCP o de UDP, no hay necesidad de configurar reglas de grupo de seguridad y reglas de ACL de red para permitir el tráfico desde la subred backend donde el balanceador de carga se despliega en los servidores backend.
3. Compruebe si se establece una conexión de TCP entre el balanceador de carga y el cliente. El tiempo de espera para una conexión de TCP es de 300s y no se puede cambiar. Si la duración excede de 300s, el balanceador de carga envía un mensaje RST al cliente y al servidor backend para desconectar la conexión.
4. Compruebe si las sesiones adhesivas están habilitadas y si el tipo de sesión adhesiva está establecido en la dirección IP de origen. En caso afirmativo, compruebe si la dirección IP de la solicitud cambia antes de que la solicitud llegue al balanceador de carga.

   Por ejemplo, si ELB se combina con Content Delivery Network (CDN) o Web Application Firewall (WAF), la dirección IP de la solicitud cambia cuando pasa con CDN o WAF. El cambio de dirección IP provoca que falle la adherencia de la sesión. Si desea utilizar CDN o WAF, se recomienda que agregue un oyente de HTTP o de HTTPS y configure sesiones adhesivas basadas en cookies.

5. Compruebe si el oyente es un oyente de HTTP o de HTTPS y las sesiones adhesivas están habilitadas. En caso afirmativo, compruebe si la solicitud contiene una cookie. Las sesiones adhesivas en la capa 7 se basan en cookies. Si la solicitud contiene una cookie, compruebe si el valor de la cookie cambia.
6. Compruebe la duración de adherencia configurada para el grupo de servidores backend. Si se habilitan las sesiones adhesivas, la duración predeterminada de la adherencia del grupo de servidores backend en la capa 4 y la capa 7 es de 20 minutos. Después de que se agote el tiempo de duración de la pegajosidad, la conexión se desconectará.
7. Compruebe si los servidores a los que accede están asociados con un balanceador de carga.

   Si **Transfer Client IP Address** está habilitado para oyentes de TCP o de UDP, no se puede usar un servidor en la nube como servidor backend y cliente.
8. Compruebe si ha agregado un servidor backend en una VPC que es diferente de aquella en la que se está ejecutando el balanceador de carga, mediante la dirección IP del servidor. En caso afirmativo, compruebe si se ha establecido una interconexión de VPC entre las dos VPC.
9. Compruebe si su cuenta está en mora. Si su cuenta está en mora, recursos como las EIP se congelarán y no se podrán utilizar.

2.3 ¿Cómo puedo manejar los códigos de error?

Los códigos de error comunes incluyen 400, 403, 502 y 504. Si se devuelve alguno de estos códigos, se recomienda que acceda al servidor backend para comprobar si puede responder correctamente.

Si el servidor backend responde correctamente, rectifique el error haciendo referencia a **Tabla 2-1**. Si el fallo persiste, póngase en contacto con servicio al cliente.

Tabla 2-1 Códigos de error comunes

Código de error	Descripción	Causas posibles
400	Error en la solicitud	● El cliente envió una solicitud mal formada que no cumple con la especificación de HTTP. ● Se envió una solicitud de HTTP al puerto de HTTPS. ● El tamaño del encabezado de solicitud excedió 64 KB.
401	Sin autorización	Error en la autenticación en el servidor backend. (Este código de error es devuelto al cliente por el servidor backend.)
403	Prohibida	La solicitud fue interceptada por el servidor backend. (Este código de error es devuelto al cliente por el servidor backend.)
404	No se ha encontrado	● El servidor backend es anormal o la aplicación no existe. (Este código de error es devuelto al cliente por el servidor backend.) ● La política de reenvío se configuró incorrectamente y la solicitud no se enrutó al servidor backend correcto.

Código de error	Descripción	Causas posibles
408	Tiempo de espera de solicitud	El cliente no envió la solicitud dentro del tiempo que el servidor se configuró para esperar, que es 60s de forma predeterminada. El envío de un paquete de mantenimiento de TCP no impide este tiempo de espera.
413	Carga útil demasiado grande	El tamaño del cuerpo de la solicitud enviado por el cliente superó los 10 GB.
414	URI demasiado largo	La URL de solicitud o el parámetro de cadena de consulta enviado por el cliente era demasiado largo.
499	Cliente ha cerrado la conexión	El cliente se desconecta del balanceador de carga antes de recibir una respuesta del balanceador de carga. Este código de error se registra solo en los registros de acceso.
500	Error del servidor interno	Hay un error interno. (Este código de error es devuelto al cliente por el servidor backend.)
501	No implementado	El balanceador de carga no pudo identificar la solicitud. El valor del campo de encabezado **Transfer-Encoding** no es **chunked** ni **identity**.
502	Gateway incorrecto	● El puerto utilizado por el servidor backend se configuró incorrectamente. ● El balanceador de carga recibió un paquete TCP RST del servidor backend cuando intentaba establecer una conexión con o enviar datos al servidor backend. ● El formato de la respuesta del servidor backend era incorrecto o la respuesta contenía un encabezado de respuesta de HTTP no válido. ● El servidor backend está configurado incorrectamente, por ejemplo, rutas o ACL de red incorrectas.
503	Servicio no disponible	La aplicación o el servidor backend no estaban disponibles. Generalmente, este código de error es devuelto por el servidor backend.
504	Tiempo de espera del gateway	● Durante la primera conexión, el balanceador de carga no puede conectarse al servidor backend antes de que se agote el tiempo de conexión. (El tiempo de espera predeterminado es de 5 segundos). ● El balanceador de carga estableció una conexión con el servidor backend, pero no respondió antes de que transcurriera el tiempo de espera de respuesta (que es 300s por defecto). ● La ACL de red de la subred no permitía al balanceador de carga acceder a los servidores backend de la subred.

3 Funcionalidad de ELB

3.1 ¿Se puede usar ELB por separado?

ELB no se puede utilizar solo.

ELB distribuye el tráfico entrante a varios servidores backend según la política de reenvío para equilibrar las cargas de trabajo. Por lo tanto, puede ampliar las capacidades de servicio externo de sus aplicaciones y eliminar los puntos únicos de falla (SPOF) para mejorar la disponibilidad del servicio. Para utilizar un balanceador de carga, debe asociar servidores backend (como ECS) con él.

3.2 ¿ELB admite las conexiones persistentes?

Sí.

Las conexiones entre el cliente y el balanceador de carga son conexiones persistentes. Después de establecer una conexión persistente de TCP, el cliente envía continuamente solicitudes HTTP al balanceador de carga hasta que se agote el tiempo de conexión. La reutilización de conexiones de TCP reduce los costes de un gran número de conexiones cortas.

3.3 ¿ELB admite FTP en servidores backend?

ELB no admite File Transfer Protocol (FTP), pero admite Secure File Transfer Protocol (SFTP) en servidores backend.

3.4 ¿Puede ELB bloquear ataques de DDoS y proteger el código web?

- ELB no proporciona funciones de seguridad como el bloqueo de ataques de DDoS.
- Anti-DDoS está habilitado para los servicios en la nube de forma predeterminada, y todo el tráfico entrante en la red pública está protegido.

NOTA

También puede utilizar Advanced Anti-DDoS (AAD), una versión avanzada de Anti-DDoS. AAD proporciona direcciones IP de alta defensa para ocultar las direcciones IP del servidor de origen, de modo que sus aplicaciones puedan resistir ataques de DDoS más grandes y sofisticados, asegurando la continuidad del servicio. Puede configurar un registro DNS para asignar las direcciones IP del servidor de origen a direcciones de alta defensa para desviar el tráfico de ataques maliciosos, proteger los servidores de origen contra ataques y evitar interrupciones en sus cargas de trabajo. Este servicio se puede desplegar en hosts utilizados en Huawei Cloud, otras nubes y centros de datos locales.

3.5 ¿Se asigna una EIP exclusivamente a un balanceador de carga?

Durante el ciclo de vida de un balanceador de carga, la EIP puede estar libre del balanceador de carga. Si la EIP no está vinculada, el balanceador de carga se convierte en un balanceador de carga de red privada, y la EIP puede estar vinculada a otros recursos.

3.6 ¿Cuántos balanceadores de carga y oyentes puedo tener?

De forma predeterminada, cada cuenta puede tener hasta 50 balanceadores de carga y 100 oyentes. Si necesita más balanceadores de carga u oyentes, aplique para aumentar sus cuotas.

Todos los balanceadores de carga de su cuenta comparten la misma cuota para los oyentes.

3.7 ¿Qué tipos de API proporciona ELB? ¿Qué son los permisos de ELB?

ELB admite las siguientes políticas:

Tabla 3-1 Políticas de ELB

Tipo de política	Nombre de la política	Descripción
Política de RBAC	Administrador de ELB	Tiene todos los permisos en ELB. Antes de asignar la política de RBAC a un grupo de usuarios, compruebe si el grupo de usuarios tiene una política dependiente. En caso afirmativo, establezca el permiso dependiente para que la política de RBAC surta efecto.
Política de grano fino	ELB FullAccess	Tiene todos los permisos en ELB. Si esta función no está habilitada, no puede asignar una política detallada a un grupo de usuarios.
	ELB ReadOnlyAccess	Tiene el permiso de solo lectura en ELB.

Tabla 3-2 Operaciones comunes respaldadas por políticas definidas por el sistema

Operación	ELB FullAccess	ELB ReadOnlyAccess	Administrador de ELB
Crear un balanceador de carga	Se admite	No se admite	Se admite
Consultar un balanceador de carga	Se admite	Se admite	Se admite
Consultar un balanceador de carga y recursos asociados	Se admite	Se admite	Se admite
Consultar los balanceadores de carga	Se admite	Se admite	Se admite
Modificación de un balanceador de carga	Se admite	No se admite	Se admite
Eliminar un balanceador de carga	Se admite	No se admite	Se admite
Agregar un oyente	Se admite	No se admite	Se admite
Consultar un oyente	Se admite	Se admite	Se admite
Modificar un oyente	Se admite	No se admite	Se admite
Eliminar un oyente	Se admite	No se admite	Se admite
Agregar un grupo de servidores de backend	Se admite	No se admite	Se admite
Consultar un grupo de servidores backend	Se admite	Se admite	Se admite
Modificar un grupo de servidores backend	Se admite	No se admite	Se admite
Eliminar un grupo de servidores backend	Se admite	No se admite	Se admite
Agregar un servidor de backend	Se admite	No se admite	Se admite
Consultar un servidor de backend	Se admite	Se admite	Se admite
Modificar un servidor de backend	Se admite	No se admite	Se admite
Eliminar un servidor de backend	Se admite	No se admite	Se admite
Configurar una comprobación de estado	Se admite	No se admite	Se admite

Operación	ELB FullAccess	ELB ReadOnlyAccess	Administrador de ELB
Consultar una comprobación de estado	Se admite	Se admite	Se admite
Modificar una comprobación de estado	Se admite	No se admite	Se admite
Deshabilitar una comprobación de estado	Se admite	No se admite	Se admite
Asignar un EIP	No se admite	No se admite	Se admite
Vincular un EIP a un balanceador de carga	No se admite	No se admite	Se admite
Consultar un EIP	Se admite	Se admite	Se admite
Desvincular un EIP de un balanceador de carga	No se admite	No se admite	Se admite
Consultar Métricas	No se admite	No se admite	Se admite
Consultar logs de acceso	No se admite	No se admite	Se admite

NOTA

- Para desvincular un EIP, también necesita configurar los permisos **vpc:bandwidths:update** y **vpc:publicIps:update** del servicio VPC. Para obtener más información, consulta la *Referencia de la API de Virtual Private Cloud*.
- Para ver las métricas de supervisión, también debe configurar el permiso **CES ReadOnlyAccess**. Para obtener más información, consulta la *Referencia de la API de Cloud Eye*.
- Para ver los registros de acceso, también necesita configurar el permiso **LTS ReadOnlyAccess**. Para obtener más información, consulta la *Referencia de la API del Log Tank Service*.

Para obtener más información acerca de los permisos detallados, consulte la *Referencia de la API de Elastic Load Balance*.

3.8 ¿Puedo ajustar el número de servidores backend cuando se está ejecutando un balanceador de carga?

Puede ajustar el número de servidores backend asociados con un balanceador de carga en cualquier momento. También puede cambiar el tipo de servidores backend según sus necesidades de servicio. Para garantizar la estabilidad del servicio, asegúrese de que las comprobaciones de estado sean normales y de que al menos un servidor backend sano esté asociado con el balanceador de carga.

3.9 ¿Pueden los servidores backend ejecutar diferentes sistemas operativos?

Sí.

ELB no restringe los sistemas operativos de los servidores backend siempre y cuando las aplicaciones en estos servidores sean las mismas y los datos sean consistentes. Sin embargo, se recomienda que instale el mismo sistema operativo en servidores backend para simplificar la gestión.

3.10 ¿Puedo configurar diferentes puertos backend para un balanceador de carga?

Sí. Puede configurar diferentes puertos backend para servidores backend asociados con un balanceador de carga.

3.11 ¿Se puede usar ELB en todas las cuentas o VPC?

- Los balanceadores de carga compartidos no pueden ser utilizados por otra cuenta y no puede asociar servidores backend cuyas VPC no son las mismas que los balanceadores de carga.
- Para balanceadores de carga dedicados, puede agregar servidores en una VPC conectada mediante una interconexión de VPC, en una VPC en otra región y conectada con una conexión en la nube, o en un centro de datos local en el otro extremo de una conexión de Direct Connect o de VPN. mediante el uso de sus direcciones IP. Para obtener más información, consulte Descripción de direcciones IP como servidores backend.

3.12 ¿Pueden los servidores backend acceder a los puertos de un balanceador de carga?

No. Los servidores backend no pueden acceder a los puertos del balanceador de carga con los que están asociados.

3.13 ¿Puedo vincular una dirección IP pública comprada de un proveedor de nube de terceros a mi balanceador de carga?

No.

Solo puede vincular una EIP comprada en Huawei Cloud a su balanceador de carga.

3.14 ¿Pueden tanto el oyente como el grupo de servidores de backend usar HTTPS?

Los balanceadores de carga dedicados admiten esta función.

Puede seleccionar HTTPS como el protocolo del oyente y el protocolo del grupo de servidores backend. Para obtener más información sobre cómo agregar un oyente, consulte **Adición de un oyente de HTTPS**.

3.15 ¿Puedo cambiar la VPC y la subred de mi balanceador de carga?

No puede cambiar la VPC y la subred de los balanceadores de carga compartidos.

Puede cambiar la subred pero no la VPC para sus balanceadores de carga dedicados.

3.16 ¿Puedo actualizar un balanceador de carga compartido a un balanceador de carga dedicado sin interrumpir el enrutamiento del tráfico?

No. Los balanceadores de carga compartidos no se pueden actualizar a balanceadores de carga dedicados.

3.17 ¿ELB admite redes IPv6?

Los balanceadores de carga compartidos solo admiten redes IPv4. Los balanceadores de carga dedicados del balanceador de carga admiten redes IPv4 e IPv6.

En la capa 4, cuando un cliente se comunica con un balanceador de carga dedicado usando una dirección IPv6, el balanceador de carga debe comunicarse con servidores backend usando una dirección IPv6. En la capa 7, cuando un cliente se comunica con un balanceador de carga dedicado usando una dirección IPv6, el balanceador de carga debe comunicarse con servidores backend usando una dirección IPv4.

NOTA

- Si no habilita IPv6 para la subred de backend especificada al crear un balanceador de carga dedicado, el balanceador de carga no puede usar direcciones IPv6 para enrutar solicitudes.
- Si necesita redes IPv6, debe seleccionar una subred backend con IPv6 habilitado para su balanceador de carga dedicado.

Figura 3-1 Tipos de red compatibles con balanceadores de carga dedicados en la capa 4

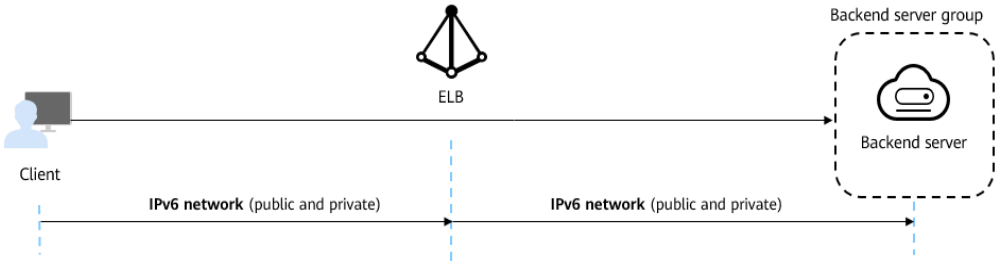
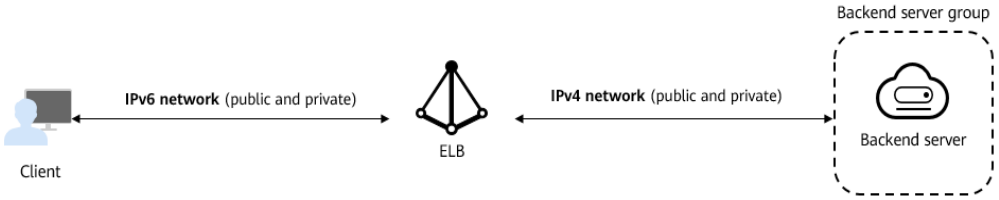


Figura 3-2 Tipos de red compatibles con balanceadores de carga dedicados en la capa 7



4 Rendimiento de equilibrio de carga

4.1 ¿Cómo puedo determinar el tiempo de respuesta del servidor basado en los datos y logs de supervisión?

Para el equilibrio de carga de HTTP y de HTTPS, puede ver el tiempo promedio de respuesta del servidor con la métrica de supervisión y ver el tiempo de respuesta de cada solicitud de los registros de acceso.

1. En la consola de ELB, haga clic en el nombre del balanceador de carga.
2. En la página de pestaña **Monitoring**, seleccione un oyente de HTTP o de HTTPS agregado al balanceador de carga.
3. Compruebe la métrica **Average Server Response Time** para ver el tiempo promedio que los servidores backend responden a las solicitudes enrutadas por el balanceador de carga.

   Tabla 4-1 Tiempo de respuesta promedio

Métrica	Definición
Tiempo de respuesta promedio del servidor	Tiempo promedio en que los servidores backend responden a las solicitudes del balanceador de carga (Esta métrica solo está disponible cuando el protocolo frontend es HTTP o HTTPS.) El proceso se inicia cuando el balanceador de carga enruta las solicitudes a los servidores backend y finaliza cuando recibe respuestas de los servidores backend. Unidad: ms

4. Compruebe los **registros de acceso** para ver el tiempo de respuesta de cada solicitud.

Los campos **request_time**, **upstream_connect_time**, **upstream_header_time** o **upstream_response_time** del log de acceso reflejan el tiempo necesario para que un balanceador de carga enrute una solicitud al servidor backend correspondiente.

Tabla 4-2 Descripción del parámetro

Campo	Descripción
request_time	Tiempo de procesamiento de la solicitud en segundos, es decir, la duración desde el memento en que el balanceador de carga recibe el primer paquete de solicitud del cliente hasta el memento en que el balanceador de carga envía el paquete de respuesta
upstream_connect_time	Tiempo necesario para establecer una conexión con el servidor, en segundos con una resolución de milisegundos Cuando el balanceador de carga intente volver a intentar una solicitud, habrá varios tiempos de conexión. Si la solicitud no se enruta correctamente al servidor backend, se muestra un guion (-) como valor nulo para este campo.
upstream_header_time	Tiempo necesario para recibir el encabezado de respuesta del servidor, en segundos con una resolución de milisegundos Cuando el balanceador de carga intenta volver a intentar una solicitud, habrá varios tiempos de respuesta. Si la solicitud no se enruta correctamente al servidor backend, se muestra un guion (-) como valor nulo para este campo.
upstream_response_time	Tiempo necesario para recibir la respuesta del servidor, en segundos con una resolución de milisegundos Cuando el balanceador de carga intenta volver a intentar una solicitud, habrá varios tiempos de respuesta. Si la solicitud no se enruta correctamente al servidor backend, se muestra un guion (-) como valor nulo para este campo.

4.2 ¿Cómo puedo comprobar si hay incoherencias de tráfico?

Compruebe si hay solicitudes fallidas en los clientes, especialmente cuando se devuelven los códigos de estado de *4xx*. Una posible causa es que las solicitudes no se enrutan a los servidores backend porque ELB considera que estas solicitudes son anormales.

4.3 ¿Cómo puedo verificar si el tráfico está siendo distribuido uniformemente?

1. Compruebe si las sesiones adhesivas están habilitadas. Si las sesiones adhesivas están habilitadas y hay pocos clientes, el tráfico puede estar distribuido de manera desigual.
2. Compruebe el estado de los servidores backend, especialmente aquellos cuyo estado cambia con el tiempo. Si un servidor backend es de **Unhealthy** o su estado cambia entre **Healthy** y **Unhealthy**, el tráfico está desequilibrado.
3. Compruebe si se utiliza el algoritmo **Source IP hash**. Si se utiliza el algoritmo, las solicitudes enviadas desde la misma dirección IP se enrutan al mismo servidor backend, lo que resulta en tráfico desequilibrado.

4. Compruebe si las aplicaciones en el servidor backend utilizan keepalive para mantener conexiones persistentes de TCP. Si se usa keepalive, el tráfico puede estar desequilibrado porque el número de solicitudes en conexiones persistentes es diferente.
5. Compruebe si se asignan las ponderaciones diferentes a los servidores backend. El tráfico varía según las ponderaciones.

NOTA

En general, además del algoritmo de equilibrio de carga, los factores que afectan el equilibrio de carga incluyen el tipo de conexión, la adherencia de sesión y las ponderaciones de servidor.

4.4 ¿Cómo puedo comprobar si hay un retraso excesivo en el acceso?

1. Vincule una EIP a un servidor backend para que las aplicaciones sean accesibles desde Internet y luego verifique el retardo de acceso. De esta manera, puede determinar si el problema es causado por el cliente, el balanceador de carga o las aplicaciones.
2. Compruebe el tráfico entrante. Si el tráfico entrante excede el ancho de banda de EIP, puede haber congestión y pérdida de paquetes.

   NOTA

   Si el tráfico entrante excede el ancho de banda disponible, no significa que el ancho de banda se utilice completamente. En este caso, necesita realizar operaciones adicionales para localizar el fallo o aumentar el ancho de banda.
3. Compruebe las políticas de carga y seguridad de los servidores backend. Si los servidores backend están muy cargados o tienen políticas de seguridad configuradas, no pueden responder rápidamente a las solicitudes del balanceador de carga asociado.
4. Compruebe la métrica **Unhealthy Servers** para ver los estados de estado de los servidores backend. Si las aplicaciones son inestables y el tiempo de espera de las conexiones al servidor backend, el mecanismo de reintento enrutará las solicitudes a otro servidor backend. Como resultado, el acceso a las aplicaciones será exitoso, pero habrá más retraso en el acceso.
5. Si el problema persiste, póngase en contacto con el servicio de atención al cliente.

4.5 ¿Qué hago si un balanceador de carga falla una prueba de esfuerzo?

1. Compruebe la carga de servidores backend. Si su uso de vCPU alcanza el 100%, las aplicaciones pueden tener cuellos de botella de rendimiento.
2. Compruebe el tráfico entrante. Si el tráfico de ráfagas excede el ancho de banda establecido para la EIP, se perderá un gran número de paquetes y no se responderá a las solicitudes, afectando de este modo al rendimiento del balanceador de carga.

   NOTA

   Si el tráfico de ráfagas excede el ancho de banda disponible, no significa que el ancho de banda se utilice completamente. En este caso, necesita realizar operaciones adicionales para localizar el fallo o aumentar el ancho de banda.
3. Compruebe el número de conexiones cortas en el estado **time_wait** en los clientes. Una posible causa es que no hay suficientes puertos de cliente.

4. El retraso de la cola de escucha de los servidores backend puede estar lleno. Si esto sucede, el servidor backend no responderá a los paquetes de SYN ACK, y el cliente se agotará el tiempo de espera. Puede aumentar el máximo permitido del retraso ajustando el parámetro **net.core.somaxconn**.

5 Balanceadores de carga

5.1 ¿Qué es la cuota?

¿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.

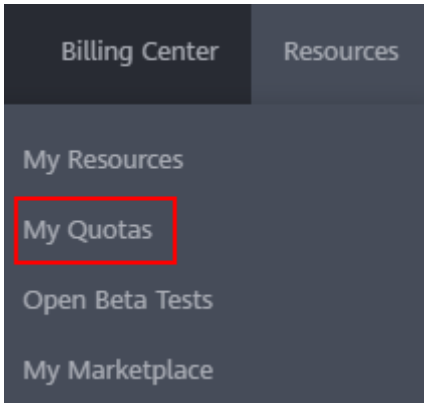
Si la cuota de recursos existente no puede cumplir con los requisitos de servicio, puede solicitar una cuota más alta.

¿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 5-1 Mis cuotas

4. Vea la cuota usada y total de cada tipo de recursos en la página mostrada.

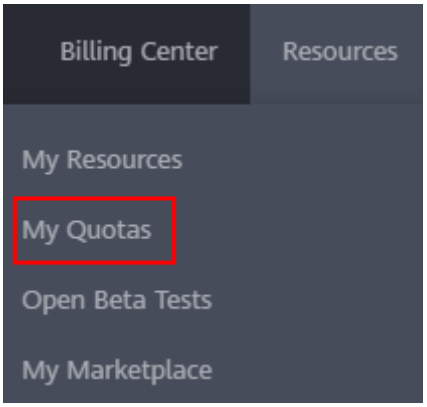
   Si una cuota no puede cumplir con los requisitos de servicio, solicite una cuota más alta.

¿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 5-2 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**.

5.2 ¿Cómo distribuye ELB el tráfico?

ELB utiliza FullNAT para reenviar el tráfico entrante. Para el equilibrio de carga en la capa 4, LVS reenvía el tráfico entrante a los servidores backend directamente. Para el equilibrio de carga en la capa 7, LVS reenvía el tráfico entrante a Nginx, que luego reenvía el tráfico a los servidores backend.

NOTA

En FullNAT, LVS traduce las direcciones IP de origen y las direcciones IP de destino de los clientes.

Figura 5-3 Equilibrio de carga en la capa 4

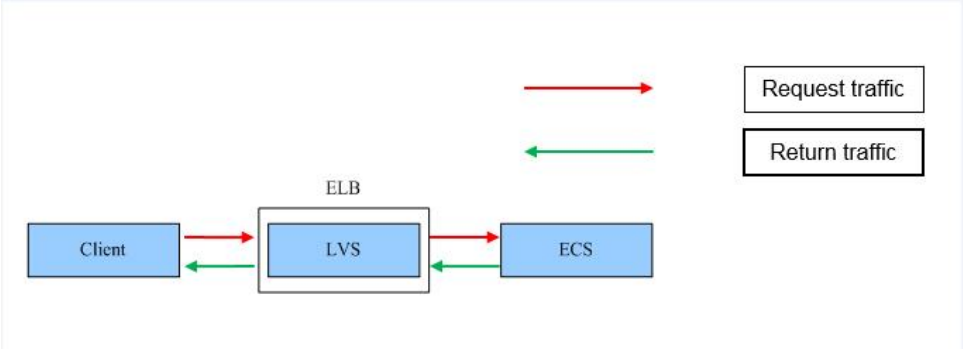
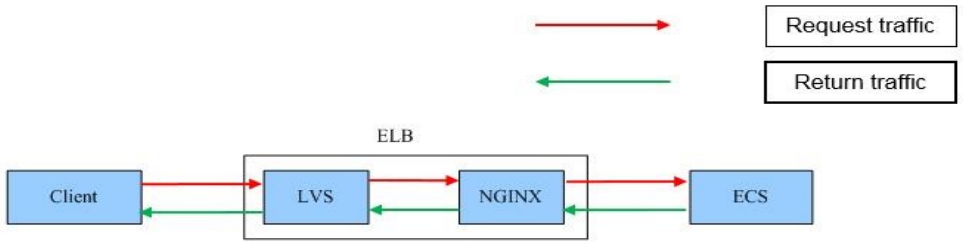


Figura 5-4 Equilibrio de carga en la capa 7



5.3 ¿Cómo puedo acceder a un balanceador de carga en todas las VPC?

VPC Peering puede ayudarle a lograr esto. Por ejemplo, si otro usuario ha creado el balanceador de carga ELB01 en VPC01, y usted está en VPC02 y desea acceder a ELB01, solo tiene que configurar una interconexión de VPC entre VPC01 y VPC02 y agregar una ruta para la conexión.

5.4 ¿Cómo puedo configurar el equilibrio de carga para aplicaciones en contenedores?

Puede configurar el equilibrio de carga mediante cualquiera de las siguientes opciones:

- Consola de gestión
- comandos de kubectl

Para obtener más información, véase **LoadBalancer**.

5.5 ¿Necesito configurar el ancho de banda de EIP para mis balanceadores de carga?

Si utiliza un balanceador de carga en una red privada, no es necesario configurar el ancho de banda de EIP. Solo necesita vincular una EIP y configurar el ancho de banda si está utilizando un balanceador de carga en una red pública.

5.6 ¿Puedo vincular varias EIP a un balanceador de carga?

No.

- Si desea utilizar el balanceador de carga en una red pública, solo puede vincular una EIP al balanceador de carga para recibir solicitudes de Internet.
- Si desea utilizar el balanceador de carga en una VPC, vincula una dirección IP privada. Para enrutar solicitudes desde una VPC diferente, debe crear una interconexión de VPC entre la VPC donde funciona el balanceador de carga y la otra VPC. Para obtener más

información, consulte la sección "Creación de una conexión de pares de VPC con otra VPC en su cuenta" en la *Guía de usuario de Virtual Private Cloud*.

5.7 ¿Por qué se requieren varias direcciones IP al crear o habilitar un balanceador de carga dedicado?

Estas direcciones IP son utilizadas por los recursos subyacentes.

Generalmente, se requieren 2 direcciones IP para crear un balanceador de carga en una singular AZ, y se requieren 6 direcciones IP para crear un balanceador de carga con IP como un backend habilitado. Si crea un balanceador de carga en varias AZ, se requerirán más direcciones IP. Existe un algoritmo para determinar cuántas direcciones IP se requieren.

5.8 ¿Por qué las solicitudes de la misma dirección IP se enrutan a diferentes servidores backend cuando el algoritmo de equilibrio de carga es hash de IP de origen?

Una posible causa es que el servidor backend que recibe las peticiones del cliente se haya vuelto insalubre. El algoritmo de hash IP de origen utiliza la dirección IP de origen de cada solicitud como una clave hash para enrutar el tráfico de un cliente particular al mismo servidor backend, siempre y cuando esté disponible. Esto permite que las solicitudes de diferentes clientes se enruten en función de sus direcciones IP de origen y garantiza que un cliente dado siempre se dirija al mismo servidor backend.

Sin embargo, si un servidor backend se vuelve insalubre y luego se recupera, ELB generará una nueva clave hash basada en la dirección IP de origen de la solicitud y los números del servidor backend. Como resultado, las solicitudes de la misma dirección IP se enrutan a diferentes servidores backend.

5.9 ¿Pueden los servidores backend acceder a Internet con la EIP del balanceador de carga?

No.

El balanceador de carga utiliza la EIP para recibir solicitudes de Internet y encamina las solicitudes a servidores backend a través de una red privada.

Si desea que los servidores backend accedan a Internet o proporcionen servicios accesibles a Internet directamente, puede vincular una EIP a cada servidor backend. También puede configurar un gateway de NAT para los servidores backend para que puedan compartir una EIP para acceder a Internet.

5.10 ¿Los balanceadores de carga compartidos tienen especificaciones?

No.

Los balanceadores de carga compartidos comparten recursos subyacentes y el rendimiento de un balanceador de carga se ve afectado por otros balanceadores de carga. Solo los

balanceadores de carga dedicados tienen uso exclusivo de sus recursos subyacentes. El rendimiento de un balanceador de carga dedicado no se ve afectado por otros balanceadores de carga dedicados en Internet.

5.11 ¿Se interrumpirá el enrutamiento de tráfico si se cambia el algoritmo de equilibrio de carga?

No. Si se cambia el algoritmo de equilibrio de carga, las conexiones establecidas no se verán afectadas. Por lo tanto, el encaminamiento del tráfico no se interrumpirá.

5.12 ¿Cuál es la diferencia entre el ancho de banda incluido en cada especificación de un balanceador de carga dedicado y el ancho de banda de una EIP?

El ancho de banda incluido en las especificaciones de los balanceadores de carga dedicados es el límite superior del tráfico entrante o saliente. 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.

5.13 ¿Cómo puedo combinar ELB y WAF?

Después de conectar su sitio web al Web Application Firewall (WAF), puede configurar el control de acceso en ELB para permitir solo el tráfico desde las direcciones IP de origen WAF a los servidores de origen. Esto evita que los piratas informáticos obtengan las direcciones IP del servidor de origen y luego omitan WAF para atacar a los servidores de origen. Para obtener más información, consulte la **Guía del usuario de Web Application Firewall**.

6 Oyentes

6.1 ¿Cuáles son las relaciones entre los algoritmos de equilibrio de carga y los tipos de sesión adhesiva?

ELB admite tres tipos de sesiones adhesivas que pueden enviar solicitudes desde el mismo cliente al mismo servidor backend. En las siguientes tablas se enumeran los tipos de sesiones adhesivas correspondientes a cada algoritmo de equilibrio de carga.

Tabla 6-1 Sesiones adhesivas compatibles con balanceadores de carga dedicados

Algoritmo de equilibrio de carga	Tipo de sesión adhesiva	Capa 4 (TCP/UDP)	Capa 7 (HTTP/HTTPS)
Round robin ponderado	Dirección IP de origen	Se admite	No se admite
	Cookie de balanceador de carga	N/A	Se admite
	Cookie de aplicación	N/A	No se admite
Conexiones mínimas ponderadas	Dirección IP de origen	No se admite	No se admite
	Cookie de balanceador de carga	N/A	No se admite
	Cookie de aplicación	N/A	No se admite
Hash de IP de origen	Dirección IP de origen	N/A	No se admite
	Cookie de balanceador de carga	N/A	No se admite
	Cookie de aplicación	N/A	No se admite

Tabla 6-2 Sesiones adhesivas compatibles con balanceadores de carga compartidos

Algoritmo de equilibrio de carga	Tipo de sesión adhesiva	Capa 4 (TCP/UDP)	Capa 7 (HTTP/HTTPS)
Round robin ponderado	Dirección IP de origen	Se admite	No se admite
	Cookie de balanceador de carga	N/A	Se admite
	Cookie de aplicación	N/A	Se admite
Conexiones mínimas ponderadas	Dirección IP de origen	No se admite	No se admite
	Cookie de balanceador de carga	N/A	No se admite
	Cookie de aplicación	N/A	No se admite
Hash de IP de origen	Dirección IP de origen	N/A	No se admite
	Cookie de balanceador de carga	N/A	No se admite
	Cookie de aplicación	N/A	No se admite

Generalmente, se recomienda el algoritmo de round robin ponderado. Las sesiones adhesivas en la capa 4 usan direcciones IP de origen para las sesiones principales, y las sesiones adhesivas en la capa 7 usan cookies de balanceador de carga.

6.2 ¿Puedo vincular varios certificados a un oyente?

Puede configurar varios certificados para un oyente de HTTPS habilitando SNI para que se puedan usar diferentes certificados para la autenticación en función de los nombres de dominio de las solicitudes.

Para obtener más información, consulte **Certificado de SNI (para oyentes de HTTPS)**.

6.3 ¿ELB dejará de distribuir el tráfico inmediatamente después de que se elimine un oyente?

- Si se elimina un oyente TCP o UDP, el balanceador de carga detiene inmediatamente el tráfico de enrutamiento porque el cliente utiliza conexiones cortas para comunicarse con el balanceador de carga.
- Si se elimina un oyente de HTTP o de HTTPS, las conexiones persistentes que se han establecido entre el cliente y el balanceador de carga se mantendrán activas hasta que se agote el tiempo de espera, por lo que el enrutamiento de solicitudes no se verá afectado. Después del tiempo de espera de las conexiones, el cliente deja de enviar solicitudes a través de estas conexiones. La duración predeterminada del tiempo de espera es 300s.

NOTA

La duración durante la cual las conexiones persistentes se mantienen activas se denomina tiempo de espera inactivo, y esto solo tiene efecto para las conexiones persistentes establecidas entre el cliente y el balanceador de carga.

6.4 ¿Tiene ELB restricciones en la velocidad y el tamaño de carga de archivos?

- ELB no tiene restricciones sobre la velocidad de carga de archivos en los clientes. Sin embargo, el ancho de banda puede limitar la velocidad de carga.
- Para los oyentes de HTTP o de HTTPS, el tamaño máximo del archivo es de 10 GB. Sin embargo, los oyentes TCP o UDP no tienen límite en el tamaño del archivo.

6.5 ¿Pueden varios balanceadores de carga enrutar las solicitudes a un servidor backend?

Sí. Esto se admite siempre que los balanceadores de carga estén en la misma subred que el servidor backend.

6.6 ¿Cómo se usa WebSocket?

Para los oyentes de HTTP, se admite WebSocket sin cifrar (ws://) de forma predeterminada. Para los oyentes de HTTPS, se admite WebSocket cifrado (wss://) de forma predeterminada.

6.7 ¿Por qué no puedo seleccionar el grupo de servidores backend de destino al agregar o modificar un oyente?

El protocolo del grupo de servidores backend (protocolo backend) que desea seleccionar no es compatible con el protocolo oyente (protocolo frontend). Hay algunas restricciones en el protocolo backend cuando asocia un grupo de servidores backend con un oyente.

Tabla 6-3 Protocolos frontend y backend de balanceadores de carga dedicados

Protocolo frontend	Protocolo backend
TCP	TCP
UDP	UDP/QUIC
HTTP	HTTP
HTTPS	HTTP/HTTPS

Tabla 6-4 Protocolos frontend y backend de balanceadores de carga compartidos

Protocolo frontend	Protocolo backend
TCP	TCP
UDP	UDP
HTTP	HTTP
HTTPS	HTTP

6.8 ¿Por qué no puedo agregar un oyente a un balanceador de carga dedicado?

Si selecciona equilibrio de carga de red (TCP/UDP) o equilibrio de carga de aplicaciones (HTTP/HTTPS) al crear el balanceador de carga, solo puede agregar oyentes del protocolo coincidente.

El tipo de equilibrio de carga no se puede cambiar después de haber sido seleccionado. Por ejemplo, si ha seleccionado el equilibrio de carga de red durante la creación del balanceador de carga, no puede cambiarlo a equilibrio de carga de aplicación y no puede agregar oyentes de HTTP o de HTTPS.

Tabla 6-5 Protocolos y tipos de equilibrio de carga

Tipo de equilibrio de carga	Protocolo	Tipos de oyentes
Equilibrio de carga de red	TCP/UDP	Oyentes de TCP y de UDP
Equilibrio de carga de aplicaciones	HTTP/HTTPS	Oyentes de HTTP y de HTTPS

7 Servidores backend

7.1 ¿Por qué el intervalo en el que los servidores backend reciben paquetes de comprobación de estado es diferente de lo que he configurado?

Cada nodo de LVS y de Nginx del sistema de ELB envía paquetes de detección a los servidores backend en el intervalo de comprobación de estado que ha especificado para el grupo de servidores backend.

Durante este período, los servidores backend reciben múltiples paquetes de detección de los nodos de LVS y de Nginx. Esto hace que parezca que los servidores backend están recibiendo paquetes a intervalos más cortos que el intervalo de comprobación de estado especificado.

7.2 ¿Pueden los servidores backend acceder a Internet después de estar asociados con un balanceador de carga?

Sí. Los servidores backend pueden acceder a Internet tanto si están asociados con un balanceador de carga.

7.3 ¿Puede ELB distribuir el tráfico entre servidores que no son proporcionados por Huawei Cloud?

- Balanceadores de carga compartidos: Los servidores backend solo pueden ser servidores en la nube de Huawei Cloud. Para obtener más información, consulte *Servidores backend*.
- Puede agregar servidores en una VPC conectada mediante una interconexión de VPC, en una VPC en otra región y conectada mediante una conexión a la nube, o en un centro de datos local en el otro extremo de una conexión de Direct Connect o de VPN, mediante sus direcciones IP. Para obtener más información, consulte **Servidores backend**Servidores backend.
- Las instancias de base de datos no se pueden utilizar como servidores backend.

- Los servidores backend no pueden funcionar en modo activo/en espera.

7.4 ¿Por qué se accede con frecuencia a los servidores backend mediante direcciones IP en 100.125.0.0/16?

Las direcciones IP en 100.125.0.0/16 son direcciones IP internas utilizadas por los balanceadores de carga para comunicarse con los servidores backend. Los balanceadores de carga utilizan estas direcciones IP como direcciones de origen para enrutar el tráfico a los servidores backend y para comprobar el estado de los servidores backend, si ha habilitado la comprobación de estado.

Para asegurarse de que su balanceador de carga puede proporcionar servicios correctamente, asegúrese de que los grupos de seguridad que contienen los servidores backend permiten el tráfico de 100.125.0.0/16.

7.5 ¿Puede ELB enrutar el tráfico a través de regiones?

- Los balanceadores de carga compartidos no pueden distribuir el tráfico entre regiones.
- Los balanceadores de carga dedicados pueden distribuir el tráfico entre regiones o VPC.
  - Para agregar servidores backend en diferentes regiones, 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 *Configuración de equilibrio de carga híbrido*.

7.6 ¿Cada servidor backend necesita una EIP para recibir solicitudes de un balanceador de carga de red pública?

No. No hay necesidad de vincular una EIP a cada servidor backend porque el balanceador de carga enruta las solicitudes con la red privada.

7.7 ¿Cómo puedo comprobar las condiciones de red de un servidor backend?

1. Compruebe que se ha asignado una dirección IP a la NIC principal del servidor.
   a. Inicie sesión en el servidor. (Un ECS se usa como ejemplo aquí.)
   b. Utilice **ifconfig** o **ip address** para ver la dirección IP.

      NOTA

      Para ECS de Windows, utilice **ipconfig** en la CLI.
2. Haga ping al gateway de la subred donde reside el ECS para comprobar la conectividad de red.
   a. En la página de detalles de la VPC, busque la subred y vea la dirección de gateway en la columna **Gateway**. Generalmente, la dirección del gateway termina con **.1**.

b. Haga ping al gateway desde el ECS. Si el gateway no se puede hacer ping, compruebe las redes en la Capa 2 y la Capa 3.

7.8 ¿Cómo puedo comprobar la configuración de red de un servidor backend?

1. Compruebe si el grupo de seguridad del servidor está configurado correctamente.
   a. En la página de detalles del servidor, vea el grupo de seguridad.
   b. Compruebe si las reglas del grupo de seguridad permiten el acceso desde el intervalo de direcciones IP correspondiente.
      - Balanceadores de carga dedicados: Compruebe si el grupo de seguridad del servidor backend tiene reglas entrantes para permitir el tráfico desde la VPC donde funciona el balanceador de carga. Si el tráfico no está permitido, agregue una regla de entrada para permitir el tráfico desde la VPC al servidor backend.
      - Balanceadores de carga Compartidos: Compruebe si el grupo de seguridad del servidor backend tiene reglas entrantes para permitir el tráfico de 100.125.0.0/16. Si no se permite el tráfico, agregue una regla de entrada para permitir el tráfico de 100.125.0.0/16 al servidor backend.

   ⚠ ATENCIÓN

   - Balanceadores de carga compartidos: Si **Transfer Client IP Address** está habilitada para un oyente de TCP o de UDP, no es necesario configurar reglas de grupo de seguridad y reglas de ACL de red para permitir el tráfico de 100.125.0.0/16 y direcciones IP del cliente a los servidores backend.
   - Balanceadores de carga dedicados: Si **IP as a Backend** no está habilitado para un balanceador de carga que tiene un oyente de TCP o de UDP, no hay necesidad de configurar reglas de grupo de seguridad y reglas de ACL de red para permitir el tráfico desde la subred backend donde el balanceador de carga se despliega en los servidores backend.

2. Asegúrese de que las ACL de red de la subred donde reside el servidor no intercepten el tráfico.

   En el panel de navegación de la consola de VPC, elija **Access Control** > **Network ACLs** y compruebe si la subred permite el tráfico.

7.9 ¿Cómo puedo comprobar el estado de un servidor backend?

1. Verifique que las aplicaciones en el servidor backend estén habilitadas.
   a. Inicie sesión en el servidor backend. (Un ECS se usa como ejemplo aquí.)
   b. Compruebe el estado del puerto.

      netstat -ntpl

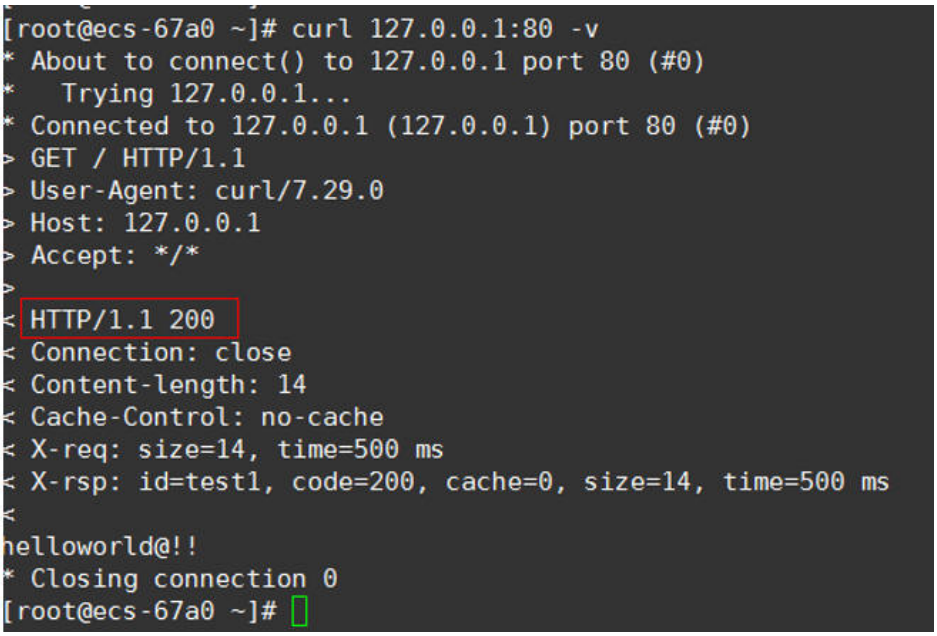
NOTA

Para ECS de Windows, utilice **netstat -ano** en la CLI para ver el estado del puerto o el estado del software del servidor.

Figura 7-1 Estado del puerto

2. Compruebe la comunicación de red del ECS.

   Por ejemplo, si el ECS utiliza el puerto 80, utilice **curl** para comprobar si la conectividad de red es normal.



7.10 ¿Cuándo se considera saludable un servidor backend?

Cuando un servidor backend se asocia con un balanceador de carga por primera vez, el servidor backend se considera saludable después de una comprobación de estado. Después de esto, el servidor se considera saludable solo después de que se ha intentado el número máximo de comprobaciones de estado.

7.11 ¿Cómo puedo comprobar si se puede acceder a un servidor backend por una EIP?

1. Vincule una EIP al servidor backend.

   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  y elija **Computing** > **Elastic Cloud Server**.
d. Localice el ECS y haga clic en su nombre.
e. En **EIPs**, haga clic en **Bind EIP**.
f. Seleccione la EIP que desea vincular y haga clic en **OK**.

2. Verifique que se pueda acceder al ECS por la EIP.

Para los ECS de Linux, utilice **curl**. Para ECS de Windows, utilice un navegador.

7.12 ¿Por qué el número de conexiones activas monitorizadas por Cloud Eye difiere del número de conexiones establecidas con los servidores backend?

El número de conexiones activas recopiladas por Cloud Eye se refiere al número de conexiones activas entre los clientes y el balanceador de carga.

Para un oyente de TCP o UDP, el balanceador de carga transmite de forma transparente las solicitudes del cliente. El número de conexiones activas es igual al número de conexiones que el balanceador de carga establece con los servidores backend.

Para un oyente de HTTP o HTTPS, los clientes se conectan al balanceador de carga, que luego se conecta a los servidores backend. El número de conexiones activas no está relacionado con el número de conexiones establecidas con los servidores backend.

7.13 ¿Por qué puedo acceder a los servidores backend después de configurar una lista blanca?

La lista blanca solo controla el acceso a un oyente. Solo las direcciones IP de la lista blanca pueden acceder al oyente. Para controlar el acceso a los servidores backend, puede configurar ACL de red o reglas de grupo de seguridad.

7.14 ¿Cuándo entrarán en vigor las ponderaciones modificadas?

Las nuevas ponderaciones para servidores backend tienen efecto 5 segundos después de configurar las ponderaciones.

- Los oyentes de TCP y UDP reenvían solicitudes sobre nuevas conexiones basadas en las nuevas ponderaciones. Sin embargo, las conexiones que se hayan establecido con servidores backend no se verán afectadas.
- Los oyentes de HTTP y HTTPS reenvían solicitudes basadas en las nuevas ponderaciones. Sin embargo, las solicitudes que se hayan reenviado a los servidores backend no se verán afectadas.

NOTA

Si la ponderación de un servidor backend se cambia a 0, la nueva ponderación no entra en vigor inmediatamente, y las solicitudes todavía se encaminan a este servidor backend. 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 conexión.

- Oyentes de TCP y de UDP: Las conexiones persistentes se desconectan después de que expire el tiempo de espera inactivo.
- Oyentes de HTTP y HTTPS: Las conexiones persistentes se desconectan después de que expire el tiempo de espera de respuesta.

7.15 ¿Por qué la subred donde reside el balanceador de carga debe tener al menos 16 direcciones IP disponibles para habilitar IP como backend?

Estas direcciones IP son utilizadas por el sistema de ELB. En general, se requieren dos direcciones IP para crear un balanceador de carga dedicado en una singular AZ, y se requieren seis direcciones IP para crear un balanceador de carga dedicado con IP como backend habilitado. Si crea un balanceador de carga dedicado en varias AZ, se necesitarán más direcciones IP. Existe un algoritmo para calcular cuántas direcciones IP se requieren.

8 Comprobaciones de estado

8.1 ¿Cómo soluciono problemas de un servidor backend insalubre?

Síntoma

Si un cliente no puede acceder a un servidor backend con un balanceador de carga, el servidor backend se declara no saludable. Puede ver los resultados de la comprobación de estado de un servidor backend en la consola de ELB.

- Balanceadores de carga dedicados

  En la página **Load Balancers**, haga clic en el nombre del balanceador de carga para ver sus detalles. Haga clic en **Backend Server Groups** y busque el grupo de servidores. Puede encontrar los resultados de la comprobación de estado de los servidores backend en el área **Basic Information**.

- Balanceadores de carga compartidos:

  En la página **Load Balancers**, haga clic en el nombre del balanceador de carga para ver sus detalles. Haga clic en **Backend Server Groups** y busque el grupo de servidores. Puede encontrar los resultados de la comprobación de estado de los servidores backend en el área **Basic Information**.

Antecedentes

Para comprobar el estado de los servidores backend, los balanceadores de carga dedicados usan las direcciones IP de la subred backend donde trabajan para enviar solicitudes de latidos a los servidores backend. mientras que los balanceadores de carga compartidos utilizan direcciones IP en 100.125.0.0/16.

Balanceadores de carga dedicados: Para asegurarse de que las comprobaciones de estado se pueden realizar según lo esperado, asegúrese de que se permita el tráfico desde la subred backend donde el balanceador de carga está trabajando a los servidores backend.

Balanceadores de carga compartidos: Para asegurarse de que las comprobaciones de estado se pueden realizar como se esperaba, asegúrese de que el tráfico esté permitido desde 100.125.0.0/16 a los servidores backend.

⚠ ATENCIÓN

- Las reglas de grupo de seguridad configuradas para servidores backend asociados con balanceadores de carga dedicados son diferentes de las configuradas para servidores backend asociados con balanceadores de carga compartidos.
  - Balanceadores de carga dedicados: asegúrese de que las reglas de grupo de seguridad permitan el acceso desde direcciones IP en la VPC donde reside el servidor backend. Para obtener más información acerca de cómo configurar grupos de seguridad para servidores backend asociados con balanceadores de carga dedicados, consulte **Configuración de reglas de grupo de seguridad para servidores backend (balanceadores de carga dedicados)**.
  - Balanceadores de carga compartidos: asegúrese de que el grupo de seguridad permita el tráfico desde 100.125.0.0/16 al servidor backend. Para obtener más información, consulte **Configuración de un grupo de seguridad para servidores backend (balanceadores de carga compartidos)**.

Si se considera que un servidor backend no está sano, ELB no encaminará el tráfico hasta que se declare sano de nuevo.

Si cambia la ponderación de un servidor backend sano a 0, el resultado de la comprobación de estado de este servidor se convierte en **Unhealthy**.

NOTA

- Cuando se detecta que un servidor backend no está sano, el balanceador de carga detendrá las solicitudes de enrutamiento a este servidor.
- Si las comprobaciones de estado están deshabilitadas, el balanceador de carga considerará el servidor backend de forma predeterminada en buen estado y seguirá enrutándole las solicitudes.
- Si **Transfer Client IP Address** está habilitado para oyentes de TCP y UDP de balanceadores de carga dedicados y compartidos, las direcciones IP del cliente en lugar de las direcciones IP en 100.125.0.0/16 se utilizan para comunicarse con el servidor backend.
- ELB utiliza direcciones IP en 100.125.0.0/16 para realizar comprobaciones de estado y enrutar solicitudes a servidores backend.
- El tráfico no se enrutará a un servidor backend con una ponderación de 0, por lo que el resultado de la comprobación de estado para este servidor backend no es relevante.

Solución de problemas

Las posibles causas se describen aquí en el orden de la probabilidad de que ocurran.

Compruebe estas causas una por una hasta que encuentre la causa de este problema.

NOTA

La modificación tarda un tiempo en surtir efecto después de cambiar la configuración de comprobación de estado. El tiempo requerido depende del intervalo de comprobación de estado y de la duración del tiempo de espera. Puede ver el resultado de la comprobación de estado en la lista del servidor backend del balanceador de carga de destino.

Figura 8-1 Proceso de solución de problemas

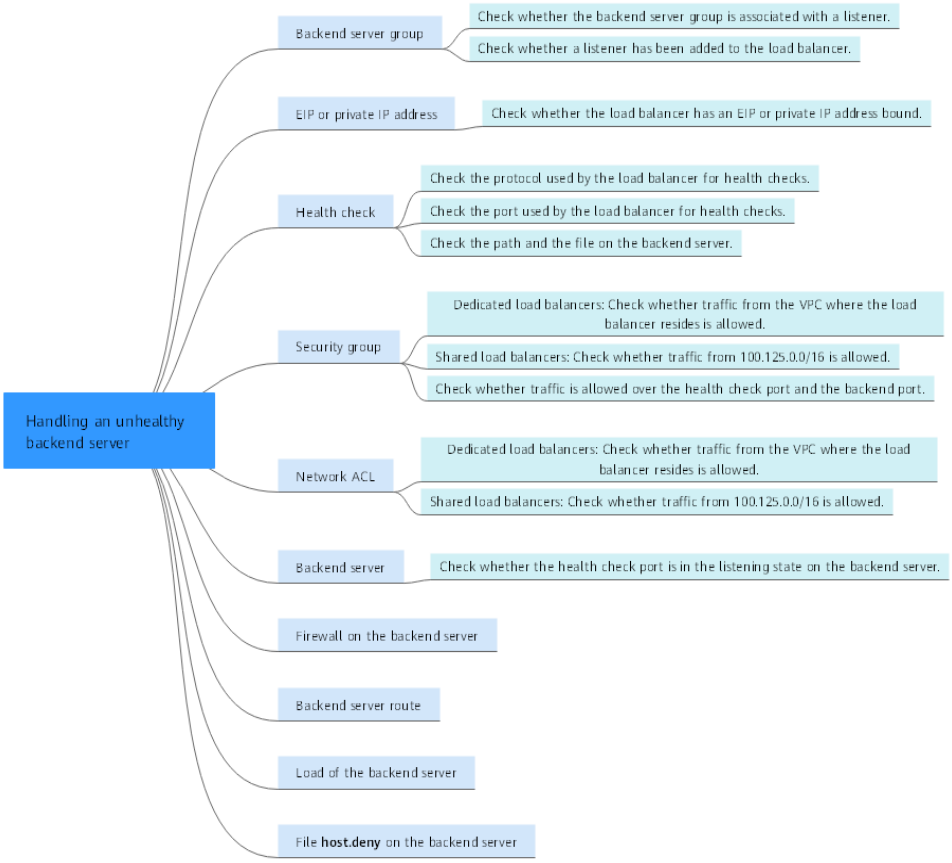


Tabla 8-1 Proceso de solución de problemas

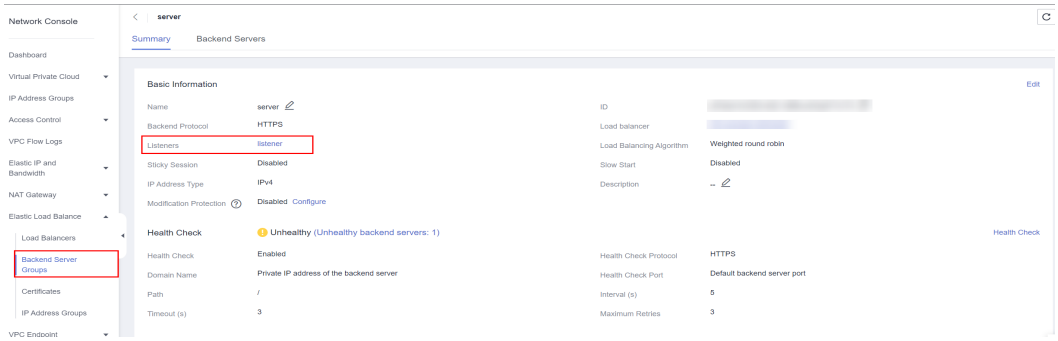
Causa posible	Solución
Grupo de servidores backend	**Comprobación de si el grupo de servidores backend está asociado con un oyente**
EIP o dirección IP privada	**Comprobación de si una EIP o una dirección IP privada están vinculadas al balanceador de carga**
Configuración de comprobación de estado	**Comprobación de la configuración de comprobación de estado**
Reglas de grupos de seguridad	**Comprobación de reglas de grupo de seguridad**
Reglas de ACL de red	**Comprobación de reglas de ACL de red**
Configuración de escucha del servidor backend	**Comprobación del servidor backend**
Reglas de ACL de red	**Checking the Firewall on the Backend Server**
Ruta del servidor backend	**Comprobación de la ruta del servidor backend**
Carga del servidor backend	**Comprobación de la carga del servidor backend**

Causa posible	Solución
Archivo **host.deny** del servidor backend	**Comprobación del archivo hosts.deny**

Comprobación de si el grupo de servidores backend está asociado con un oyente

Compruebe si el grupo de servidores backend al que pertenece el servidor backend poco saludable está asociado con un oyente.

Figura 8-2 Comprobación del oyente con el grupo de servidores backend asociado



- Si el grupo de servidores backend no está asociado con un oyente, compruebe si se ha agregado un oyente al balanceador de carga.
  - Si hay un oyente, asocia el grupo de servidores backend con el oyente.
  - Si no hay oyentes, agregue un oyente. Seleccione **Use existing** y, a continuación, seleccione el grupo de servidores backend cuando agregue el oyente.
- Si el grupo de servidores backend se ha asociado con un oyente, proceda con las siguientes operaciones.

Comprobación de si una EIP o una dirección IP privada están vinculadas al balanceador de carga

NOTA

- Compruebe esto solo cuando agregue un oyente TCP o UDP al balanceador de carga.
- Si agrega un oyente de HTTP o de HTTPS al balanceador de carga, las comprobaciones de estado no se verán afectadas sin importar si una dirección IP privada o EIP está vinculada al balanceador de carga.

Si agrega un oyente de TCP o UDP al balanceador de carga, compruebe si el balanceador de carga tiene una EIP o una dirección IP privada vinculada.

Si el balanceador de carga no tiene EIP o dirección IP privada vinculada, enlace uno.

NOTA

Cuando se crea un balanceador de carga por primera vez, si no hay una dirección IP privada o EIP vinculada al balanceador de carga, el resultado de la comprobación de estado de los servidores backend asociados con un oyente de TCP o UDP es **Unhealthy**. Después de vincular una EIP o una dirección IP privada al balanceador de carga, el resultado de la comprobación de estado se convierte en **Healthy**. Si desvincula la EIP o la dirección IP privada del balanceador de carga, el resultado de la comprobación de estado sigue siendo **Healthy**.

Comprobación de la configuración de comprobación de estado

Haga clic en el nombre del balanceador de carga para ver sus detalles. Vaya a **Backend Server Groups** y, a continuación, haga clic en el nombre del grupo de servidores. En el área **Basic Information**, a la derecha de **Health Check**, haga clic en **Configure**. Compruebe los siguientes parámetros:

- **Domain Name**: Si utiliza HTTP para las comprobaciones de estado y el servidor backend está configurado para verificar el encabezado del host, introduzca el nombre de dominio configurado para el servidor backend.
- **Protocol**: El protocolo utilizado para las comprobaciones de estado.
- **Port**: El puerto debe ser el que se usa en el servidor backend, y no se puede cambiar. Compruebe si el puerto de comprobación de estado está en el estado de escucha en el servidor backend. Si no lo es, el servidor backend se identificará como insalubre.
- **Check Path**: Si se utiliza HTTP para las comprobaciones de estado, debe comprobar este parámetro. Se recomienda un simple archivo HTML estático.

NOTA

- Si el protocolo de comprobación de estado es HTTP, el puerto y la ruta se utilizan para las comprobaciones de estado.
- Si el protocolo de comprobación de estado es TCP, solo se utiliza el puerto para las comprobaciones de estado.
- Si el protocolo de comprobación de estado es HTTP y el puerto de comprobación de estado es normal, cambie la ruta o cambie el protocolo de comprobación de estado a TCP.
- Escriba una ruta absoluta.

  Por ejemplo:

  Si la dirección URL es **http://www.example.com** o **http://192.168.63.187:9096** escriba **/** como ruta de comprobación de estado.

  Si la dirección URL es **http://www.example.com/chat/try/**, escriba **/chat/try/** como ruta de comprobación de estado.

  Si la dirección URL es **http://192.168.63.187:9096/chat/index.html**, escriba **/chat/index.html** como ruta de comprobación de estado.

Comprobación de reglas de grupo de seguridad

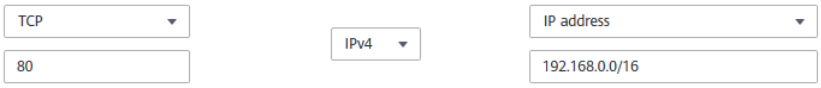
- **Balanceadores de carga dedicados**
  - **Oyentes de TCP, de HTTP o de HTTPS**: Verifique que la regla de grupo de seguridad entrante permita el tráfico TCP desde la VPC donde reside el balanceador de carga dedicado al servidor backend a través del puerto de comprobación de estado.
    - **Si el puerto de comprobación de estado es el mismo que el puerto backend**: la regla de entrada debe permitir el tráfico sobre el puerto backend, por ejemplo, el puerto 80.

- **Si el puerto (puerto 80 como ejemplo) para la comprobación de la salud es diferente del utilizado por el servidor backend (puerto 443 como ejemplo)**, las reglas de grupo de seguridad entrante deben permitir el tráfico a través de ambos puertos.

  NOTA

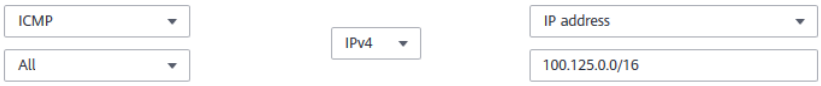
  Puede comprobar el protocolo y el puerto en el área **Basic Information** del grupo de servidores backend.

Figura 8-3 Ejemplo de regla entrante



– **Oyentes de UDP**: Verifique que la regla de grupo de seguridad entrante permita el tráfico desde la VPC donde reside el balanceador de carga dedicado al servidor backend mediante el protocolo de comprobación de estado y sobre el puerto de comprobación de estado. Además, la regla debe permitir el tráfico de ICMP entrante.

Figura 8-4 Ejemplo de regla de entrada que permite el tráfico de ICMP

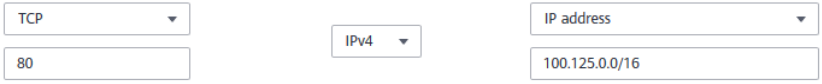


- **Balanceadores de carga compartidos**
  – **Oyentes de TCP, de HTTP o de HTTPS**: Verifique que la regla entrante del grupo de seguridad que contiene el servidor backend permita el acceso desde 100.125.0.0/16 y permite el tráfico desde el puerto de comprobación de estado.
    - **Si el puerto de comprobación de estado es el mismo que el puerto backend**: la regla de entrada debe permitir el tráfico sobre el puerto backend, por ejemplo, el puerto 80.
    - **Si el puerto (puerto 80 como ejemplo) para la comprobación de la salud es diferente del utilizado por el servidor backend (puerto 443 como ejemplo)**, las reglas de grupo de seguridad entrante deben permitir el tráfico a través de ambos puertos.

      NOTA

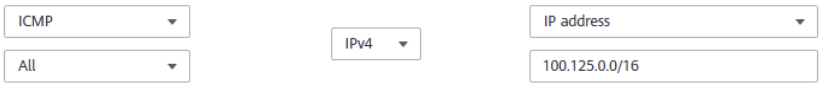
      Puede comprobar el protocolo y el puerto en el área **Basic Information** del grupo de servidores backend.

Figura 8-5 Ejemplo de regla entrante



– **Oyentes de UDP**: Verifique que la regla de grupo de seguridad entrante permita el tráfico de 100.125.0.0/16 al servidor backend mediante el protocolo de comprobación de estado y sobre el puerto de comprobación de estado. Además, la regla debe permitir el tráfico de ICMP entrante.

Figura 8-6 Ejemplo de regla de entrada que permite el tráfico de ICMP



NOTA

- Se debe permitir el acceso al servidor backend desde direcciones IP en 100.125.0.0/16. Esto se debe a que el balanceador de carga se comunica con los servidores backend utilizando estas direcciones IP. Después de enrutar el tráfico a los servidores backend, las direcciones IP de origen se convierten en direcciones IP de 100.125.0.0/16. Además, el balanceador de carga utiliza estas direcciones IP para enviar solicitudes de latidos a los servidores backend para comprobar su estado.
- Si no está seguro acerca de las reglas del grupo de seguridad, cambie el **Protocol & Port** a **All** para realizar pruebas.
- Para oyentes de UDP, véase **¿Cómo realiza ELB las comprobaciones de estado de UDP? ¿Cuáles son las precauciones para las comprobaciones de estado de UDP?**

Comprobación de reglas de ACL de red

- **Balanceadores de carga dedicados**

  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 predeterminadas de ACL de red rechazan todo el tráfico entrante y saliente. Si la subred de un balanceador de carga o de los servidores backend asociados tiene asociada una ACL de red, el balanceador de carga no puede recibir tráfico de Internet ni enrutar el tráfico a los servidores backend, y los servidores backend no pueden recibir tráfico del balanceador de carga ni responder al mismo.

  Configure una regla entrante de ACL de red para permitir el tráfico desde la VPC donde reside el balanceador de carga hacia los servidores backend.

  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 de la página y elija **Networking** > **Virtual Private Cloud**.

  d. En el panel de navegación de la izquierda, elija **Access Control** > **Network ACLs**.

  e. En la lista de ACL de red, haga clic en el nombre de la ACL de red para cambiar a la página que muestra sus detalles.

  f. En la página **Inbound Rules** o **Outbound Rules**, haga clic en **Add Rule** para agregar una regla.

     - **Action**: Seleccione **Allow**.
     - **Protocol**: El protocolo debe ser el mismo que seleccionó para el oyente.
     - **Source**: Establezca el bloque CIDR de VPC.
     - **Source Port Range**: Seleccione un rango de puertos.
     - **Destination**: Ingrese una dirección de destino permitida en esta dirección. Si mantiene el valor predeterminado **0.0.0.0/0** se permitirá el tráfico para todas las direcciones IP de destino.
     - **Destination Port Range**: Seleccione un rango de puertos.

- (Opcional) **Descripción**: Describa la regla de ACL de red si es necesario.

g. Haga clic en **OK**.

- **Balanceadores de carga compartidos**

  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 predeterminadas de ACL de red rechazan todo el tráfico entrante y saliente. Si la subred de un balanceador de carga o de los servidores backend asociados tiene asociada una ACL de red, el balanceador de carga no puede recibir tráfico de Internet ni enrutar el tráfico a los servidores backend, y los servidores backend no pueden recibir tráfico del balanceador de carga ni responder al mismo.

  Puede configurar una regla de ACL de red entrante para permitir el acceso desde 100.125.0.0/16.

  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 de la página y elija **Networking** > **Virtual Private Cloud**.

  d. En el panel de navegación de la izquierda, elija **Access Control** > **Network ACLs**.

  e. En la lista de ACL de red, haga clic en el nombre de la ACL de red para cambiar a la página que muestra sus detalles.

  f. En la página **Inbound Rules** o **Outbound Rules**, haga clic en **Add Rule** para agregar una regla.

  - **Action**: Seleccione **Allow**.
  - **Protocol**: El protocolo debe ser el mismo que seleccionó para el oyente.
  - **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. Si mantiene el valor predeterminado **0.0.0.0/0** se permitirá el tráfico para todas las direcciones IP de destino.
  - **Destination Port Range**: Seleccione un rango de puertos.
  - (Opcional) **Descripción**: Describa la regla de ACL de red si es necesario.

  g. Haga clic en **OK**.

Comprobación del servidor backend

NOTA

Si el servidor backend se ejecuta en Windows, utilice un navegador para acceder a **https://***{Backend server IP address}*:*{Health check port}*. Si se devuelve un código 2xx o 3xx, el servidor backend se está ejecutando normalmente.

- Ejecute el siguiente comando en el servidor backend para comprobar si se escucha el puerto de comprobación de estado:

```
netstat -anlp | grep port
```

  Si se muestran el puerto de comprobación de estado y el **LISTEN**, el puerto de comprobación de estado se encuentra en estado de escucha. Como se muestra en la **Figura 8-7**, se escucha en el puerto TCP 880.

Si no especifica un puerto de comprobación de estado, los puertos backend se utilizan de forma predeterminada.

Figura 8-7 Puerto del servidor backend escuchado en

Figura 8-8 No se escucha el puerto del servidor backend

Si el puerto de comprobación de estado no está en estado de escucha, el servidor backend no está en estado de escucha. Debe iniciar la aplicación en el servidor backend y comprobar si se escucha el puerto de comprobación de estado.

- Para las comprobaciones de estado HTTP, ejecute el siguiente comando en el servidor backend para comprobar el código de estado:

```
curl Private IP address of the backend server:Health check port/Health check path -iv
```

Para realizar una comprobación de estado HTTP, el balanceador de carga inicia una solicitud de GET al servidor backend. Si se muestran los siguientes códigos de estado de respuesta, el servidor backend se considera saludable:

Oyentes de TCP: 200

Balanceadores de carga dedicados: 200 para comprobaciones de estado HTTP/HTTPS

Balanceadores de carga compartidos: 200, 202 o 401 para la comprobación de estado HTTP

Figura 8-9 Servidor backend insalubre

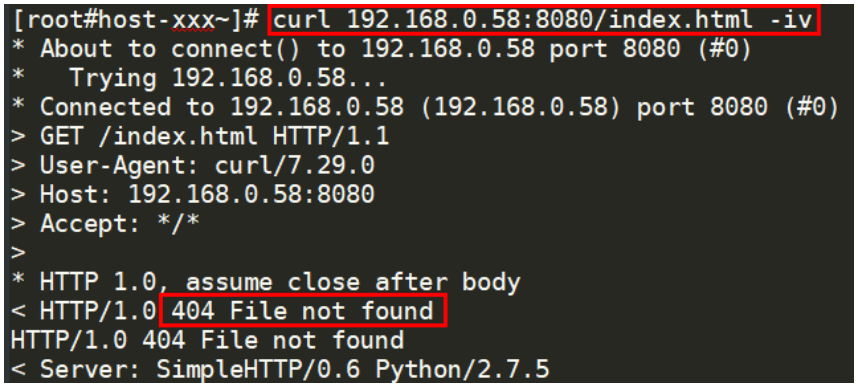
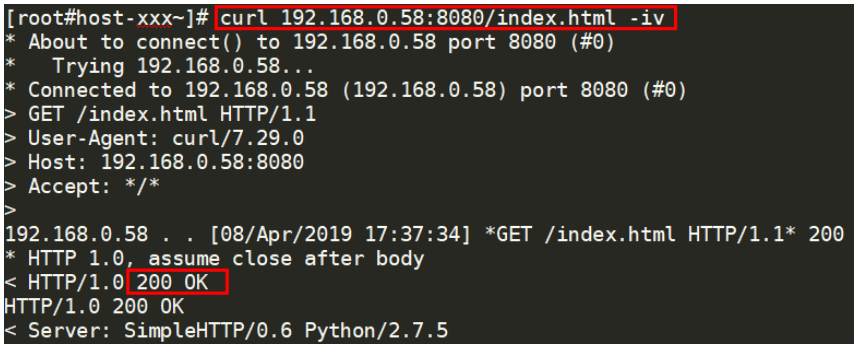


Figura 8-10 Servidor backend saludable



- Si se utiliza HTTP para las comprobaciones de estado y se detecta que el servidor backend no está en estado, realice los siguientes pasos para configurar una comprobación de estado TCP:

  En la página de ficha **Listeners**, modifique el oyente de destino, seleccione el grupo de servidores backend para el que se ha configurado la comprobación de estado TCP o agregue un grupo de servidores backend y seleccione TCP como protocolo de comprobación de estado. Después de completar la configuración, espere un tiempo y compruebe el resultado de la comprobación de estado.

Checking the Firewall on the Backend Server

Si el firewall u otro software de seguridad está habilitado en el servidor de back-end, el software puede bloquear las direcciones IP en la subred de back-end del balanceador de carga o 100.125.0.0/16.

Para los balanceadores de carga dedicados, configure las reglas de firewall entrantes para permitir el tráfico desde la subred backend donde el balanceador de carga trabaja a los servidores backend.

Para los balanceadores de carga compartidos, configure las reglas de firewall entrantes para permitir el tráfico de 100.125.0.0/16 a los servidores backend.

Comprobación de la ruta del servidor backend

Compruebe si la ruta predeterminada configurada para la NIC principal se ha modificado manualmente. Si se cambia la ruta predeterminada, es posible que los paquetes de comprobación de estado no lleguen al servidor backend.

Ejecute el siguiente comando en el servidor backend para comprobar si la ruta predeterminada apunta al gateway (Para las comunicaciones de nivel 3, la ruta predeterminada debe estar configurada para apuntar al gateway de la subred de VPC donde reside el servidor backend):

```
ip route
```

Alternativamente, ejecute el siguiente comando:

```
route -n
```

Figura 8-11 muestra la salida del comando cuando la ruta del servidor backend es normal.

Figura 8-11 Ejemplo de ruta predeterminada que apunta al gateway

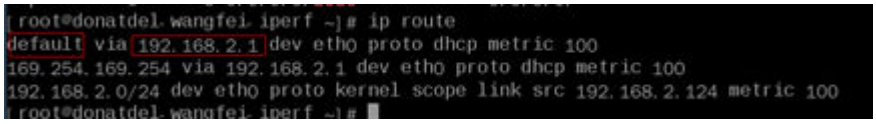
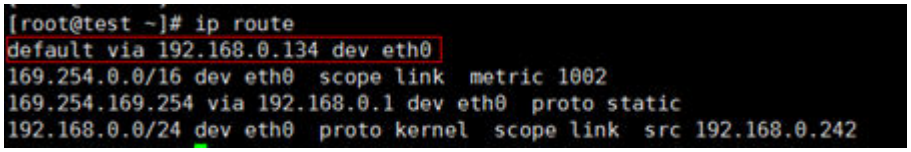


Figura 8-12 Ejemplo de ruta predeterminada que no apunta al gateway



Si la salida del comando no contiene la primera ruta, o la ruta no apunta al gateway, configure o modifique la ruta predeterminada para que apunte al gateway.

Comprobación de la carga del servidor backend

Vea el uso de la vCPU, el uso de la memoria y las conexiones de red del servidor backend en la consola de Cloud Eye para comprobar si el servidor backend está sobrecargado.

Si la carga es alta, las conexiones o las solicitudes de comprobaciones de estado pueden agotarse.

Comprobación del archivo hosts.deny

Verifique que las direcciones IP de la VPC donde funcionan los balanceadores de carga y 100.125.0.0/16 no se escriban en el archivo **/etc/hosts.deny** del servidor backend.

Para los balanceadores de carga dedicados, verifique que las direcciones IP de la VPC donde funcionan los balanceadores de carga no estén escritas en el archivo.

Para los balanceadores de carga compartidos, verifique que las direcciones IP de 100.125.0.0/16 no estén escritas en el archivo.

Envío de un ticket de servicio

Si el problema persiste, **envíe un ticket de servicio**.

8.2 ¿Por qué el intervalo en el que los servidores backend reciben paquetes de comprobación de estado es diferente del intervalo configurado?

Cada nodo de LVS y de Nginx en el sistema de ELB detecta servidores backend en el intervalo de comprobación de estado que ha especificado para el grupo de servidores backend.

Durante este período, los servidores backend reciben paquetes de detección de múltiples nodos. Esto hace que parezca que los servidores backend reciben estos paquetes a intervalos más cortos que el intervalo de comprobación de estado especificado.

8.3 ¿Cómo realiza ELB las comprobaciones de estado de UDP? ¿Cuáles son las precauciones para las comprobaciones de estado de UDP?

Cómo funcionan las comprobaciones de estado de UDP

UDP es un protocolo sin conexión. Una comprobación de estado de UDP se implementa de la siguiente manera:

- El nodo de comprobación de estado envía una solicitud de ICMP al servidor backend basada en la configuración de comprobación de estado.
  - Si el nodo de comprobación de estado recibe una respuesta ICMP del servidor backend, considera que el servidor backend está sano y continúa con la comprobación de estado.
  - Si el nodo de comprobación de estado no recibe una respuesta de ICMP del servidor backend, considera que el servidor backend no está sano.

- Después de recibir la respuesta de ICMP, el nodo de comprobación de estado envía un paquete de sondeo UDP al servidor backend.
  - Si el nodo de comprobación de estado recibe un mensaje de ICMP Port Unreachable del servidor backend dentro de la duración del tiempo de espera, el servidor backend se considera insatisfactorio.
  - Si el nodo de comprobación de estado no recibe un mensaje ICMP Port Unreachable del servidor backend dentro de la duración del tiempo de espera, el servidor backend se considera saludable.

Cuando utilice UDP para las comprobaciones de estado, conserve la configuración de parámetros predeterminada.

Solución de problemas

Si el servidor backend no está sano, utilice cualquiera de los siguientes métodos para localizar el error:

- Compruebe si el tiempo de espera es demasiado corto.

  Una posible causa es que el mensaje ICMP Echo Reply o ICMP Port Unreachable devuelto por el servidor backend no alcanza el nodo de comprobación de estado dentro de la duración del tiempo de espera. Como resultado, el resultado de la comprobación de estado es inexacto.

  Se recomienda cambiar la duración del tiempo de espera a un valor mayor.

  Las comprobaciones de estado de UDP son diferentes de otras comprobaciones de estado. Si la duración del tiempo de espera de la comprobación de estado es demasiado corta, el resultado de la comprobación de estado del servidor backend con frecuencia alterna entre **Healthy** y **Unhealthy**.
- Compruebe si el servidor backend restringe la velocidad a la que se generan los mensajes ICMP.

Para servidores de Linux, ejecute los siguientes comandos para consultar el límite de velocidad y la máscara de velocidad:

```
sysctl -q net.ipv4.icmp_ratelimit
```

El límite de velocidad predeterminado es **1000**.

```
sysctl -q net.ipv4.icmp_ratemask
```

La máscara de velocidad predeterminada es **6168**.

Si el valor devuelto del primer comando es el valor predeterminado o **0**, ejecute el siguiente comando para eliminar el límite de velocidad de los mensajes Port Unreachable:

```
sysctl -w net.ipv4.icmp_ratemask=6160
```

Para obtener más información, consulte *Linux Programmer's Manual*. En la CLI de Linux, ejecute el siguiente comando para mostrar el manual:

```
man 7 icmp
```

Si lo prefiere, visite **http://man7.org/linux/man-pages/man7/icmp.7.html**.

NOTA

Una vez que se elimina el límite de velocidad, el número de mensajes de ICMP Port Unreachable en el servidor backend no estará limitado.

Precauciones

Tenga en cuenta lo siguiente cuando configure las comprobaciones de estado de UDP:

- Las comprobaciones de estado de UDP utilizan paquetes de ping para comprobar el estado del servidor backend. Para garantizar la transmisión sin problemas de estos paquetes, asegúrese de que ICMP esté habilitado en el servidor backend realizando lo siguiente:

  Inicie sesión en el servidor y ejecute el siguiente comando como usuario **root**:

  cat /proc/sys/net/ipv4/icmp_echo_ignore_all

  – Si el valor devuelto es **1**, ICMP está deshabilitado.

  – Si el valor devuelto es **0**, ICMP está habilitado.
- El resultado de la comprobación de estado puede ser diferente del estado real del servidor backend.

  Si el servidor backend ejecuta Linux, la tasa de paquetes de ICMP puede estar limitada debido a la defensa de Linux contra ataques de ping inundación cuando hay un gran número de solicitudes simultáneas. En este caso, si se produce una excepción de servicio, el balanceador de carga no recibirá el mensaje de error **port XX unreachable** y considerará que la comprobación de estado se realiza correctamente. Como resultado, hay una inconsistencia entre el resultado de la comprobación de estado y el estado real del servidor.

8.4 ¿Por qué ELB envía frecuentemente solicitudes a servidores backend durante las comprobaciones de estado?

ELB se despliega en clústeres, y todos los nodos para el reenvío de solicitudes en el clúster envían solicitudes a los servidores backend al mismo tiempo. Si el intervalo de comprobación de estado es demasiado corto, se realizan comprobaciones de estado una vez cada pocos segundos y se envía un gran número de paquetes a los servidores backend. Para controlar la frecuencia de acceso a los servidores backend, cambie el intervalo de comprobación de estado haciendo referencia a *Modificación de una comprobación de estado*.

8.5 ¿Cuándo comienza una comprobación de estado?

Después de agregar un servidor backend a un grupo de servidores backend, la comprobación de estado se realiza en un tiempo aleatorio durante el primer intervalo y luego en el intervalo especificado.

8.6 ¿Los reintentos máximos incluyen comprobaciones de estado que consideran que los servidores backend son insalubres?

Sí. Los reintentos máximos son el número máximo de comprobaciones de estado tras las cuales se detecta que un servidor backend está sano o el número máximo de comprobaciones de estado tras las cuales se detecta que el mismo servidor backend no está sano.

8.7 ¿Qué hago si se generan muchos logs de acceso durante las comprobaciones de estado?

1. Puede aumentar el intervalo de comprobación de estado haciendo referencia a Cambio de las configuraciones de comprobación de estado.

   Riesgo: Después de que se prolongue el intervalo de comprobación de estado, el tiempo para que el balanceador de carga detecte servidores no saludables aumentará.

2. Puede deshabilitar la comprobación de estado haciendo referencia a Deshabilitar una comprobación de estado.

   Riesgo: Después de deshabilitar las comprobaciones de estado, el balanceador de carga no comprobará los servidores backend. Si un servidor backend se vuelve defectuoso, el balanceador de carga seguirá enrutando las solicitudes a este servidor.

8.8 ¿Qué códigos de estado se devolverán si los servidores backend están identificados como saludables?

Tabla 8-2 Códigos de estado de comprobación de estado

Tipo de balanceador de carga	Protocolo de comprobación de estado	Código de estado
Balanceadores de carga dedicados	HTTP	200
	HTTPS	200
Balanceadores de carga compartidos:	HTTP	● 200 ● 202 ● 401

9 Obtención de direcciones IP de origen

9.1 ¿Cómo puedo transferir la dirección IP de un cliente?

Cuando utiliza ELB para enrutar solicitudes a servidores backend, las direcciones IP de los clientes serán traducidas por ELB. Esta sección le guía para obtener las direcciones IP de los clientes.

- Equilibrio de carga en Capa 7 (oyentes de HTTP o HTTPS): Configure el servidor de aplicaciones y obtenga la dirección IP de un cliente desde el encabezado de HTTP.

  Para obtener más información, véase **Balanceo de carga de capa 7**.
- Equilibrio de carga en Capa 4 (oyentes de TCP o UDP): Utilice cualquiera de los siguientes métodos para obtener la dirección IP real de un cliente.
  - Método 1: Habilitar **Transfer Client IP Address** para los oyentes.
  - Método 2: Configurar el complemento de TOA.

  Para obtener más información, véase **Balanceo de carga de capa 4**.

Restricciones y limitaciones

- Si se utiliza Network Address Translation (NAT), no se pueden obtener las direcciones IP de los clientes.
- Si el cliente es un contenedor solo puede obtener la dirección IP del nodo donde se encuentra el contenedor, pero no puede obtener la dirección IP del contenedor.
- Si **Transfer Client IP Address** está habilitado para oyentes de TCP o UDP, no se puede usar un servidor en la nube como servidor backend y cliente al mismo tiempo.
- De forma predeterminada, la función **Transfer Client IP Address** está habilitada para los oyentes de TCP y UDP de balanceadores de carga dedicados y no se puede deshabilitar.

NOTA

Si se utilizan tanto WAF como ELB, también puede obtener las direcciones IP de los clientes con WAF. Para obtener más información, consulte la **Guía del usuario de Web Application Firewall**.

Balanceo de carga de capa 7

Configure el servidor de aplicaciones y obtenga la dirección IP de un cliente desde el encabezado de HTTP.

El balanceador de carga coloca la dirección IP real en el campo de encabezado X-Forwarded-For en el siguiente formato:

```
X-Forwarded-For: IP address of the client,Proxy server 1-IP address,Proxy server 2-IP address,...
```

Si utiliza este método, la primera dirección IP obtenida es la dirección IP del cliente.

Servidor de Apache

1. Instalar Apache 2.4.

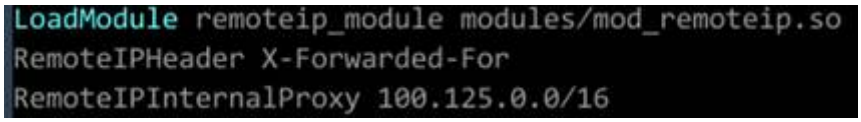
   Por ejemplo, si se utiliza CentOS 7.5 como sistema operativo, ejecute el siguiente comando para instalar el software:

   ```
   yum install httpd
   ```

2. Agregar el siguiente contenido al final del archivo de configuración de Apache **/etc/httpd/conf/httpd.conf**:

   ```
   LoadModule remoteip_module modules/mod_remoteip.so
   RemoteIPHeader X-Forwarded-For
   RemoteIPInternalProxy 100.125.0.0/16
   ```

   Figura 9-1 Contenido a agregar

   NOTA

   Agregue el rango de direcciones IP del servidor proxy después de **RemoteIPInternalProxy**.

   - Balanceadores de carga compartidos: 100.125.0.0/16 y el rango de direcciones IP utilizado por el servicio AAD. Los balanceadores de carga utilizan direcciones IP en 100.125.0.0/16 para comunicarse con servidores backend, y no hay riesgos de seguridad. Utilice la coma (,) para separar varias entradas.
   - Balanceadores de carga dedicados: bloque CIDR de la subred donde reside el balanceador de carga

3. Cambie el formato de salida del log en el archivo de configuración de Apache a lo siguiente (el **%a** indica la dirección IP de origen):

   ```
   LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
   ```

4. Reinicie Apache.

   ```
   systemctl restart httpd
   ```

5. Obtenga la dirección IP real del cliente de los registros de acceso httpd.

Servidor de Nginx

Por ejemplo, si se utiliza CentOS 7.5 como sistema operativo, ejecute el siguiente comando para instalar el software:

1. Ejecute los siguientes comandos para instalar http_realip_module:

   ```
   yum -y install gcc pcre pcre-devel zlib zlib-devel openssl openssl-devel
   wget http://nginx.org/download/nginx-1.17.0.tar.gz
   tar zxvf nginx-1.17.0.tar.gz
   ```



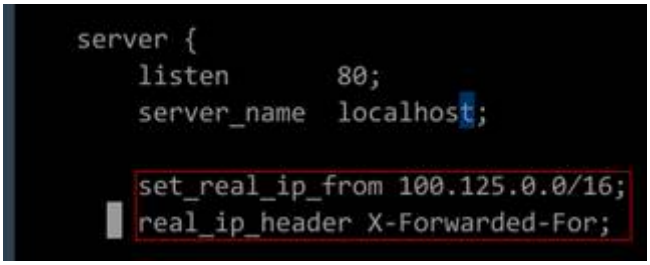
```
cd nginx-1.17.0
./configure --prefix=/path/server/nginx --with-http_stub_status_module --
without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
```

2. Ejecute el siguiente comando para abrir el archivo **nginx.conf**:
   ```
   vi /path/server/nginx/conf/nginx.conf
   ```
3. Agregue nuevos campos e información al final de la siguiente información de configuración:

   Agregue la siguiente información en **http** o **server**:

   ```
   set_real_ip_from 100.125.0.0/16;
   real_ip_header X-Forwarded-For;
   ```

   Figura 9-2 Adición de información

   NOTA

   Agregue el rango de direcciones IP del servidor proxy después de **set_real_ip_from <IP_address>**.

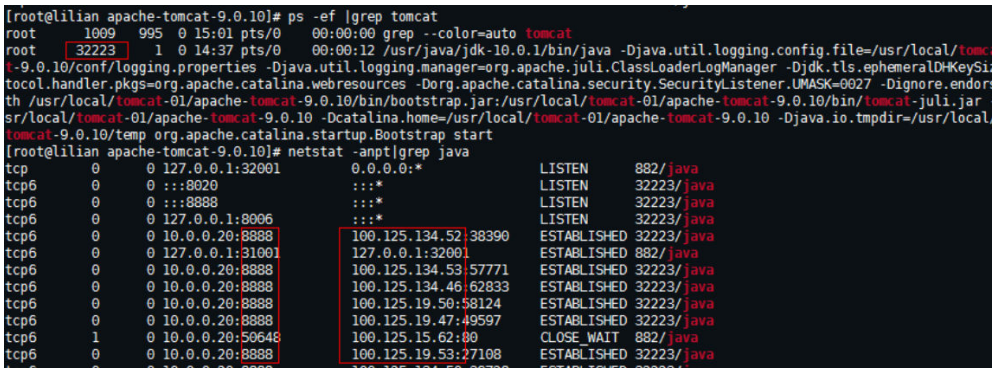
   - Balanceadores de carga compartidos: 100.125.0.0/16 y el rango de direcciones IP utilizado por el servicio AAD. Los balanceadores de carga utilizan direcciones IP en 100.125.0.0/16 para comunicarse con servidores backend, y no hay riesgos de seguridad. Utilice la coma (,) para separar varias entradas.
   - Balanceadores de carga dedicados: bloque CIDR de la subred donde reside el balanceador de carga
4. Inicie Nginx.
   ```
   /path/server/nginx/sbin/nginx
   ```
5. Obtenga la dirección IP real del cliente de los registros de acceso de Nginx.
   ```
   cat /path/server/nginx/logs/access.log
   ```

Servidor de Tomcat

En las siguientes operaciones, la ruta de instalación de Tomcat es **/usr/tomcat/tomcat8/**.

1. Inicie sesión en un servidor en el que Tomcat está instalado.
2. Compruebe si Tomcat está funcionando correctamente.
   ```
   ps -ef|grep tomcat
   netstat -anpt|grep java
   ```

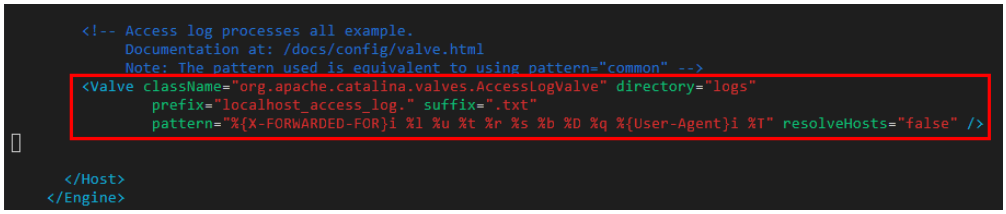

Figura 9-3 Tomcat funcionando correctamente



3. Modifique **className="org.apache.catalina.valves.AccessLogValve"** en el archivo **server.xml** de la siguiente manera:

```
vim /usr/tomcat/tomcat8/conf/server.xml
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt"
pattern="%{X-FORWARDED-FOR}i %l %u %t %r %s %b %D %q %{User-Agent}i %T"
resolveHosts="false" />
```

Figura 9-4 Ejemplo de configuración

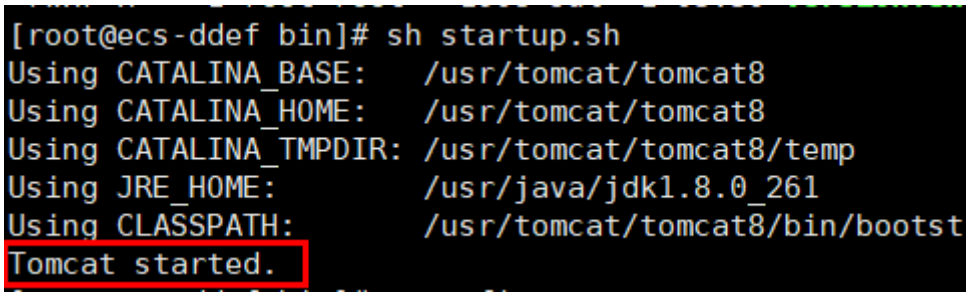


4. Reinicie el servicio de Tomcat.

```
cd /usr/tomcat/tomcat8/bin && sh shutdown.sh && sh startup.sh
```

/usr/tomcat/tomcat8/ es donde Tomcat está instalado. Cámbielo en función de los requisitos del sitio.

Figura 9-5 Reiniciar el servicio de Tomcat



5. Consulte los logs más recientes.

   Como se destaca en la siguiente figura, las direcciones IP que no están en el intervalo de direcciones IP que comienza con 100.125 son las direcciones IP de origen.

```
cd /usr/tomcat/tomcat8/logs/
cat localhost_access_log..2021-11-29.txt
```

En este comando, **localhost_access_log..2021-11-29.txt** indica la ruta de log del día actual. Cámbielo en función de los requisitos del sitio.

Figura 9-6 Consultar la dirección IP de origen

```
100.125.68.197 - - [29/Nov/2021:14:33:27 +0800] "GET /bg-upper.png HTTP/1.1" 200 3103
100.125.68.197 - - [29/Nov/2021:14:33:27 +0800] "GET /bg-middle.png HTTP/1.1" 200 1918
100.125.68.197 - - [29/Nov/2021:14:33:27 +0800] "GET /bg-button.png HTTP/1.1" 200 713
100.125.68.197 - - [29/Nov/2021:14:33:27 +0800] "GET /favicon.ico HTTP/1.1" 200 21630
100.125.68.197 - - [29/Nov/2021:14:33:38 +0800] "GET / HTTP/1.1" 200 11250
100.125.68.197 - - [29/Nov/2021:14:35:09 +0800] "GET / HTTP/1.1" 200 11250
[xxxxxxxxxxxxxxlogs]# cat localhost_access_log..2021-11-29.txt
124.7      6 - - [29/Nov/2021:14:41:09 +0800] GET / HTTP/1.1 200 11250 178  Mozilla/5.0
0.178
124.7        - - [29/Nov/2021:14:41:47 +0800] GET / HTTP/1.1 200 11250 3  Mozilla/5.0 (
003
124.7        - - [29/Nov/2021:14:42:10 +0800] GET / HTTP/1.1 200 11250 3  Mozilla/5.0 (
003
```

Windows Server con IIS desplegado

El siguiente ejemplo utiliza Windows Server 2012 con IIS7 para describir cómo obtener la dirección IP de origen.

1. Descargue e instale IIS.
2. Descargue el complemento **F5XForwardedFor.dll** y copie los complementos de los directorios **x86** y **x64** a un directorio para el que IIS tenga el permiso de acceso, por ejemplo, **C:\F5XForwardedFor2008**.
3. Abra el Server Manager y elija **Modules** > **Configure Native Modules**.

Figura 9-7 Selección de módulos

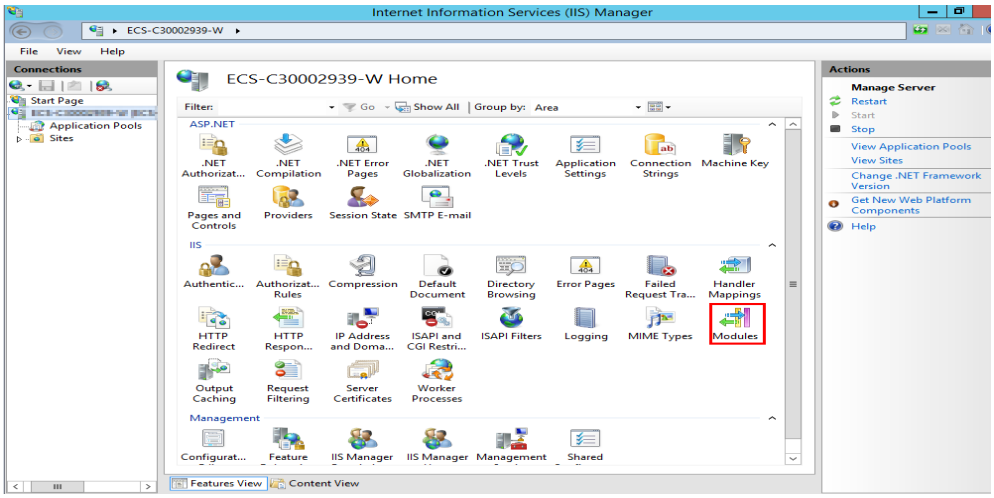
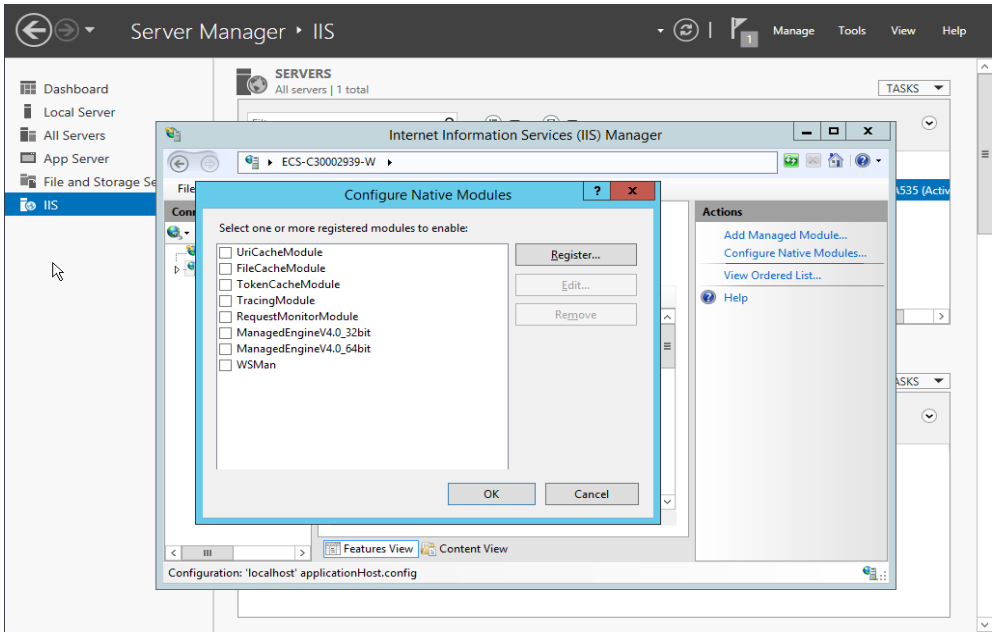
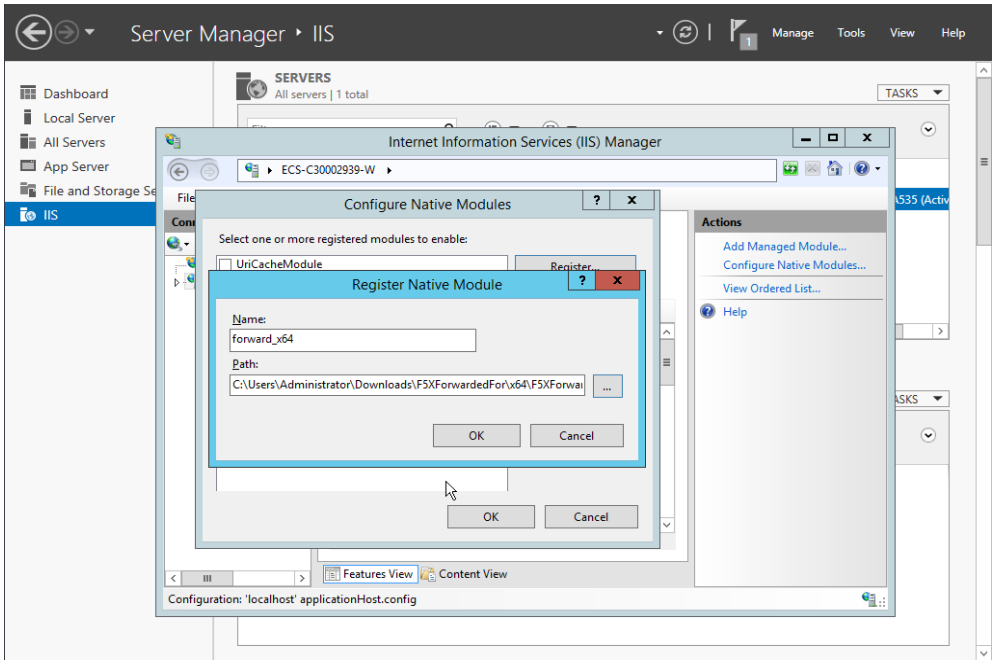


Figura 9-8 Configurar módulos nativos



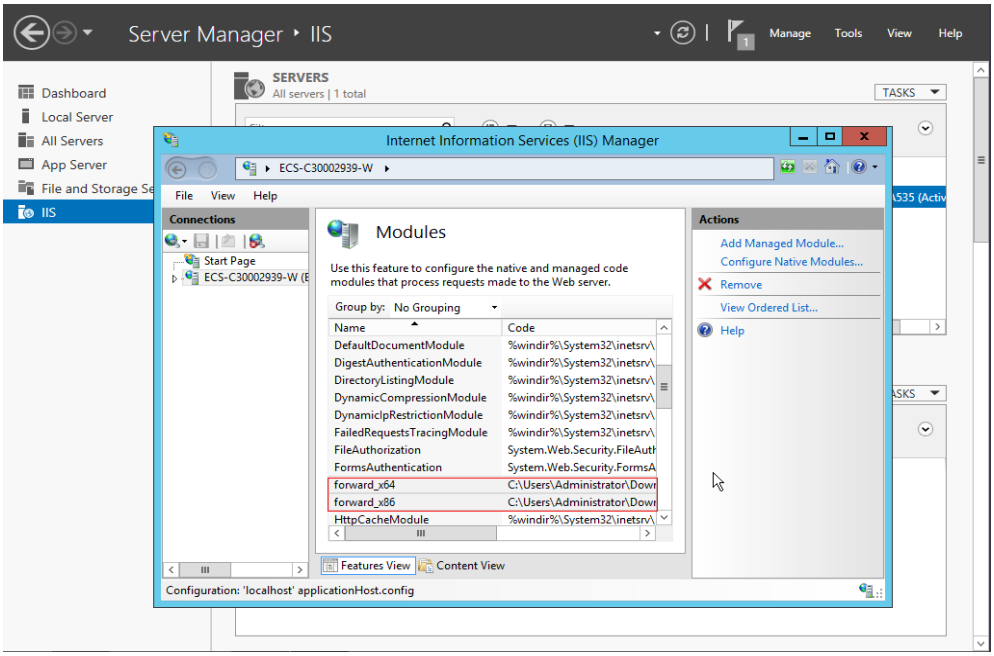
4. Haga clic en **Register** para registrar los complementos x86 y x64.

Figura 9-9 Registro de complementos



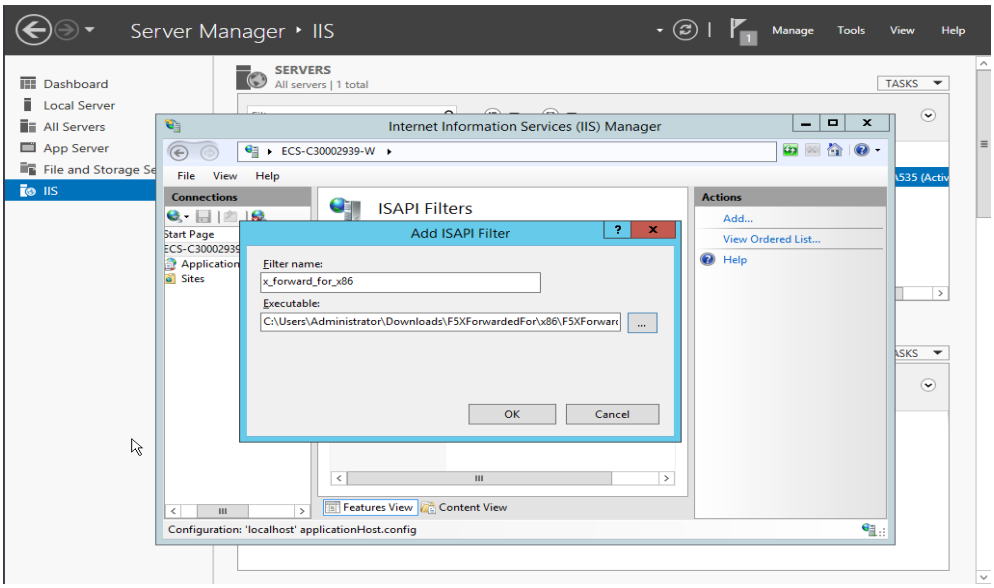
5. En el cuadro de diálogo **Modules**, compruebe que los complementos registrados se muestran en la lista.

Figura 9-10 Confirmación de la inscripción



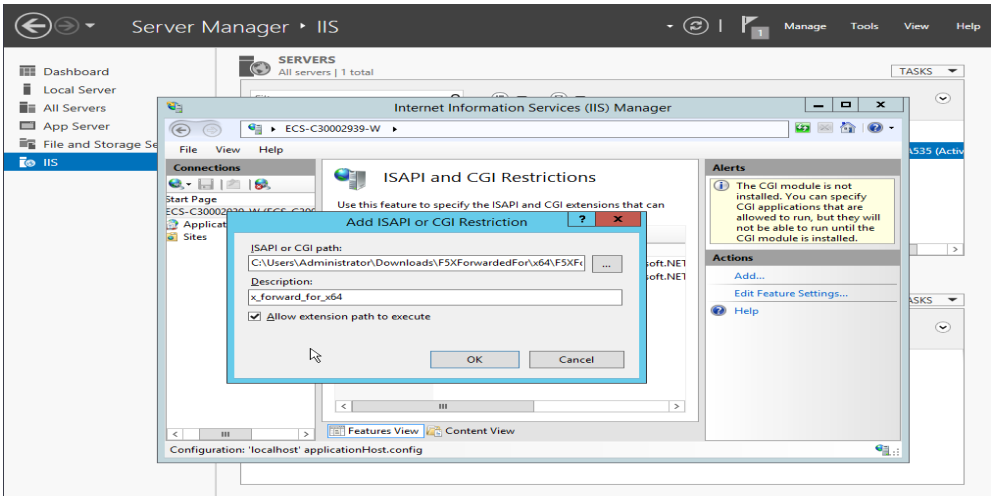
6. Seleccione **ISAPI Filters** en la página principal del Server Manager y autorice dos complementos para ejecutar extensiones ISAPI y CGI.

Figura 9-11 Adición de autorización



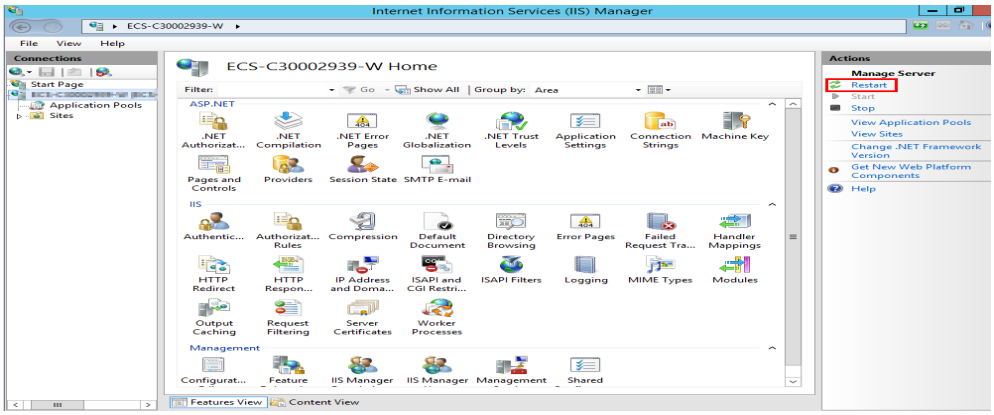
7. Seleccione **ISAPI and CGI Restriction** para establecer el permiso de ejecución para los dos complementos.

Figura 9-12 Permitir que los complementos se ejecuten



8. Haga clic en **Restart** en la página de inicio para reiniciar IIS. La configuración tendrá efecto después del reinicio.

Figura 9-13 Reinicio de IIS



Balanceo de carga de capa 4

For load balancing at Layer 4 (TCP or UDP listeners), use either of the following methods to obtain the real IP address of a client:

- **Método 1 (para oyentes de TCP o de UDP)**: Habilitar **Transfer Client IP Address**.

⚠ ATENCIÓN

- Después de habilitar esta función, el tráfico, tal como el tráfico de descarga unidireccional o push, puede interrumpirse cuando los servidores backend se están migrando durante la migración del balanceador de carga clásico asociado. Después de migrar los servidores backend, retransmita los paquetes para restaurar el tráfico.
- Una vez habilitada esta función, los servidores backend asociados no se pueden utilizar como clientes para acceder al oyente.
- 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 dos intervalos de comprobación de estado.

a. Realice los siguientes pasos para habilitar la función:
   i. Inicie sesión en la consola de gestión.
   ii. En la esquina superior izquierda de la página, haga clic en y seleccione la región y el proyecto deseados.
   iii. Pase el ratón sobre en la esquina superior izquierda para mostrar **Service List** y elija **Networking** > **Elastic Load Balance**.
   iv. En la lista del balanceador de carga, haga clic en el nombre del balanceador de carga.
   v. Haga clic en **Listeners**.
      - Para agregar un oyente, haga clic en **Add Listener**.
      - Para modificar un oyente, localice el oyente, haga clic en a la derecha de su nombre y haga clic en **Modify Listener**. En el cuadro de diálogo **Modify Listener**, modifique los parámetros según sea necesario.
   vi. Habilite **Transfer Client IP Address**.
b. Configure grupos de seguridad, ACL de red y políticas de seguridad de SO y software para que las direcciones IP de los clientes puedan acceder a estos servidores backend.

NOTA

Si habilita esta función, un servidor no puede servir como servidor backend y como cliente. Si el cliente y el servidor backend usan el mismo servidor y la opción **Transfer Client IP Address** está habilitada, el servidor backend pensará que el paquete del cliente se envía por sí mismo y no devolverá un paquete de respuesta al balanceador de carga. Como resultado, el tráfico de retorno se interrumpirá.

- **Método 2 (para oyentes de TCP)**: Configurar el complemento de TOA.

  Los oyentes de TCP requieren el complemento de TOA para obtener direcciones IP reales. Para obtener más información, consulte **Configuración del complemento de TOA**.

10 Oyentes de HTTP/HTTPS

10.1 ¿Qué protocolo debo seleccionar para el grupo de servidores backend al agregar un oyente de HTTPS?

Para usar HTTPS tanto en el frontend como en el backend, puede crear un balanceador de carga dedicado, agregar un oyente HTTPS al balanceador de carga y establecer el protocolo de backend en HTTPS.

Para usar HTTPS solo en el frontend, puede crear un balanceador de carga dedicado, agregar un oyente de HTTPS al balanceador de carga y establecer el protocolo backend en HTTP.

NOTA

El uso de HTTPS tanto en el frontend como en el backend solo le permite habilitar la autenticación mutua en el balanceador de carga y los servidores backend.

10.2 ¿Por qué hay una advertencia de seguridad después de configurar un certificado?

Lo siguiente puede causar el aviso No Secure incluso después de configurar un certificado:

- El nombre de dominio utilizado por el certificado es diferente del nombre de dominio al que acceden los usuarios. (Si este es el caso, compruebe el nombre de dominio que utilizó el certificado para asegurarse de que los nombres de dominio son los mismos o cree un certificado autofirmado.)
- El SNI está configurado, pero el nombre de dominio especificado es diferente del utilizado por el certificado.
- El nivel de nombre de dominio no es coherente con el nivel de certificado.

Si el problema persiste, ejecute el comando **curl** *{Domain name}* para localizar el error basado en la información de error devuelta por el sistema.

10.3 ¿Por qué es una política de reenvío en el estado defectuoso?

Una posible causa es que agregó una política de reenvío que es la misma que una existente. Incluso si elimina la política de reenvío existente, la nueva política de reenvío sigue siendo defectuosa.

Para resolver este problema, elimine la nueva política de reenvío y agregue una diferente.

10.4 ¿Por qué no puedo agregar una política de reenvío a un oyente?

Compruebe el protocolo de oyente.

Las políticas de reenvío solo se pueden agregar a los oyentes de HTTP y de HTTPS.

10.5 ¿Por qué no puedo seleccionar un grupo de servidores backend existente al agregar una política de reenvío?

Esto se debe a que el grupo de servidores backend ha sido utilizado por otra política de reenvío. Solo una política de reenvío puede utilizar un grupo de servidores backend.

11 Sesiones persistentes

11.1 ¿Cuáles son las diferencias entre las conexiones persistentes y las sesiones adhesivas?

Las conexiones persistentes no están necesariamente relacionadas con las sesiones adhesivas.

Una conexión persistente permite que múltiples paquetes de datos se envíen continuamente a través de una conexión TCP. Si no se envían paquetes de datos por la conexión, el cliente y el servidor necesitan enviar paquetes de detección de enlace entre sí. Las sesiones adhesivas permiten que todas las solicitudes del mismo cliente durante una sesión se envíen al mismo servidor backend.

11.2 ¿Cómo puedo comprobar si las sesiones adhesivas no surtieron efecto?

1. Compruebe si las sesiones adhesivas están habilitadas para el grupo de servidores backend. Si las sesiones adhesivas están habilitadas, vaya al siguiente paso.
2. Compruebe el resultado de la comprobación de estado del servidor backend. Si el resultado de la comprobación de estado es **Unhealthy**, el tráfico se enruta a otros servidores backend y las sesiones adhesivas no son válidas.
3. Si selecciona el algoritmo hash IP de origen, compruebe si la dirección IP de la solicitud cambia antes de que el balanceador de carga reciba la solicitud.
4. Si las sesiones adhesivas están habilitadas para un oyente de HTTP o de HTTPS, compruebe si la solicitud contiene una cookie. Si lo son, compruebe si el valor de la cookie ha cambiado (porque el equilibrio de carga en la capa 7 utiliza cookies para mantener las sesiones).

11.3 ¿Cómo pruebo sesiones adhesivas con comandos de Linux Curl?

1. Preparar los recursos necesarios.

a. Compre tres ECS, uno como cliente y los otros dos como servidores backend.

b. Cree un balanceador de carga y agregue un oyente de HTTP al balanceador de carga. Habilita las sesiones adhesivas cuando agrega el oyente.

2. Inicie el servicio HTTP de los dos servidores backend.

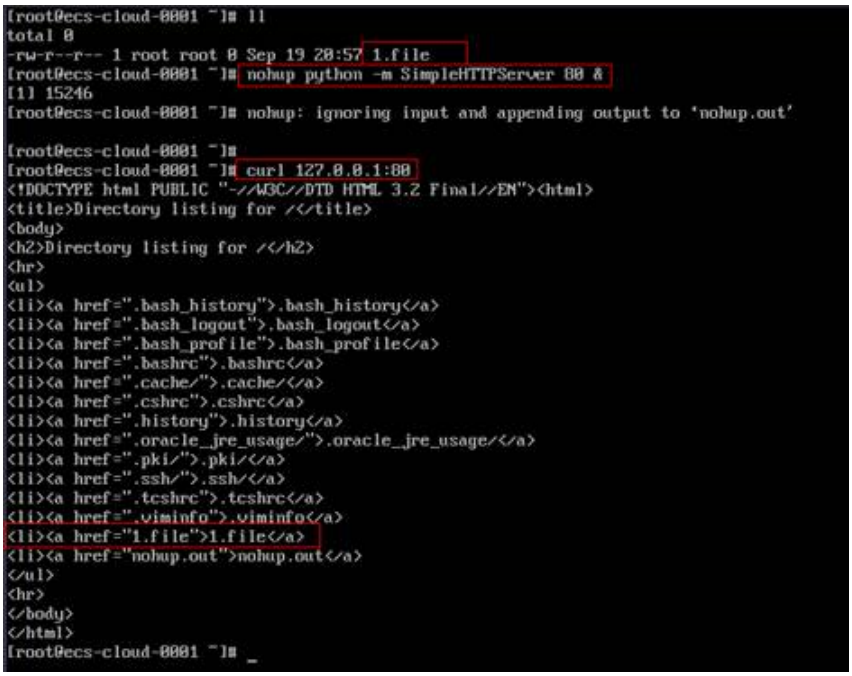
   Inicie sesión en un servidor backend y cree un archivo llamado **1.file** en el directorio actual para marcar este servidor.

   Ejecute el siguiente comando en el directorio actual para iniciar el servicio de HTTP:

   nohup python –m SimpleHTTPServer 80 &

   Ejecute el siguiente comando para comprobar si el servicio HTTP es normal:

   curl http://127.0.0.1:80



   Inicie sesión en el otro servidor backend y cree un archivo llamado **2.file** en el directorio actual.

   Ejecute el siguiente comando en el directorio actual para iniciar el servicio de HTTP:

   nohup python –m SimpleHTTPServer 80 &

   Ejecute el siguiente comando para comprobar si el servicio HTTP es normal:

   curl http://127.0.0.1:80


```
[root@ecs-cloud-0002 ~]# touch 2.file
[root@ecs-cloud-0002 ~]# nohup python -m SimpleHTTPServer 80 &
[1] 15244
[root@ecs-cloud-0002 ~]# nohup: ignoring input and appending output to 'nohup.out'

[root@ecs-cloud-0002 ~]# curl 127.0.0.1:80
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cache/">.cache/</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".oracle_jre_usage/">.oracle_jre_usage/</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
<li><a href=".viminfo">.viminfo</a>
<li><a href="2.file">2.file</a>
<li><a href="nohup.out">nohup.out</a>
</ul>
<hr>
</body>
</html>
[root@ecs-cloud-0002 ~]#
```

3. Acceda al balanceador de carga desde el cliente y especifique el valor de la cookie.

   El siguiente es un comando de ejemplo. Cambie los parámetros según sea necesario. Asegúrese de que los nombres de archivo devueltos de cada solicitud son los mismos.

   curl --cookie "name=abcd" http://ELB_IP:Port

```
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cache/">.cache/</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".oracle_jre_usage/">.oracle_jre_usage/</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
<li><a href=".viminfo">.viminfo</a>
<li><a href="2.file">2.file</a>
<li><a href="nohup.out">nohup.out</a>
</ul>
<hr>
</body>
</html>
[root@ecs-client ~]# curl --cookie "name=abcd"  http://192.168.172.242:80
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href=".bash_history">.bash_history</a>
<li><a href=".bash_logout">.bash_logout</a>
<li><a href=".bash_profile">.bash_profile</a>
<li><a href=".bashrc">.bashrc</a>
<li><a href=".cache/">.cache/</a>
<li><a href=".cshrc">.cshrc</a>
<li><a href=".history">.history</a>
<li><a href=".oracle_jre_usage/">.oracle_jre_usage/</a>
<li><a href=".pki/">.pki/</a>
<li><a href=".ssh/">.ssh/</a>
<li><a href=".tcshrc">.tcshrc</a>
<li><a href=".viminfo">.viminfo</a>
<li><a href="2.file">2.file</a>
<li><a href="nohup.out">nohup.out</a>
</ul>
<hr>
</body>
</html>
[root@ecs-client ~]# curl --cookie "name=abcd" http://192.168.172.242:80
```


11.4 ¿Qué tipos de sesiones adhesivas admite ELB?

Dedicated load balancers: **Source IP address** and **Load balancer cookie**

Balanceadores de carga compartidos: **Source IP address**, **Load balancer cookie** y **Application cookie**

12 Certificados

12.1 ¿Cómo puedo crear certificados de servidor y certificados de CA?

Consulte **Autenticación mutua** para crear certificados de servidor y certificados de CA. En general, solo es necesario autenticar los servidores backend. Solo necesita configurar certificados de servidor.

12.2 ¿ELB admite certificados comodín?

Sí. Si el nombre de dominio de un certificado comodín es *.test.com, se admiten los nombres de dominio a.test.com, b.test.com, a.b.test.com y c.d.test.com.

12.3 ¿Por qué el acceso a los servidores backend sigue siendo anormal incluso si he creado un certificado?

Las siguientes son posibles causas:

- Ha creado un certificado en la consola de ELB, pero no tiene un oyente de HTTPS.

  Para solucionar este problema, realice los siguientes pasos:

  – Continúe utilizando el oyente actual e instale el certificado en el servidor backend.

  – Eliminar el oyente actual, agregar un oyente de HTTPS, y vincular un certificado al oyente de HTTPS.
- Ha creado un certificado en la página **Certificates** y está utilizando un oyente de HTTPS, pero no ha vinculado el certificado al oyente.
- Su certificado ha caducado.
- El nombre de dominio es diferente del especificado al crear el certificado.
- Se utiliza una cadena de certificados, pero su formato es incorrecto.
- Ha vinculado un certificado al oyente de HTTPS y también ha configurado un certificado en los servidores backend. Debido a que se une un certificado al oyente, ELB descifra las solicitudes de HTTPS de los clientes y envía solicitudes descifradas a los

servidores backend, y el certificado en los servidores backend descifra estas solicitudes descifradas de nuevo. (Los balanceadores de carga compartidos tienen esta restricción, mientras que los balanceadores de carga dedicados no tienen esta restricción.)

Puede utilizar cualquiera de los métodos siguientes para resolver el problema:

– Configure un certificado en los servidores backend y use un oyente de TCP para transmitir de forma transparente el tráfico de HTTPS a los servidores backend.
– Use un oyente de HTTPS y vincule un certificado al oyente de HTTPS. No configure el certificado en los servidores backend.

12.4 ¿Se interrumpirá la red o el equilibrio de carga cuando se reemplace un certificado?

No.

El nuevo certificado entra en vigor inmediatamente después de la sustitución. El certificado antiguo se utiliza para conexiones establecidas, y el nuevo se utiliza para nuevas conexiones.

NOTA

Cuando el certificado expira, el sistema muestra un mensaje que indica que la conexión no es segura. Sin embargo, puede ignorar la advertencia y continuar accediendo al sitio web.

13 Registro de acceso

13.1 ¿Por qué no se muestran los logs de acceso para mi balanceador de carga?

- Asegúrese de que LTS se ha habilitado y de que se han creado un grupo de log y un flujo de log. Para obtener más información, consulte **Registro de acceso**.
- Asegúrese de que se pueda acceder al balanceador de carga.
- Asegúrese de que el balanceador de carga admita el registro de acceso.

  El registro de acceso se puede habilitar para los oyentes de HTTP o de HTTPS de balanceadores de carga compartidos.

13.2 ¿Qué información puedo proporcionar para ayudar al personal de O&M?

Póngase en contacto con el servicio de atención al cliente. Si ELB todavía no responde después de haber realizado las operaciones previstas en las secciones **¿Cómo puedo comprobar las condiciones de red de un servidor backend?** a **¿Cómo puedo comprobar si se puede acceder a un servidor backend por una EIP?**

Proporcionar al servicio de atención al cliente la siguiente información.

Concepto	Rellene los detalles
ID de balanceador de carga	-
ID de la VPC	-
Dirección IP del balanceador de carga	-
ID de oyente	-
Protocolo y puerto frontend	-
Protocolo y puerto de comprobación de estado	-

Concepto	Rellene los detalles
Resultado de la comprobación de estado	-
ID de ECS 1	-
ID de ECS 2	-

14 Monitoreo

14.1 ¿Por qué la tasa de salida en la consola de ELB es incompatible con las estadísticas de uso de ancho de banda en la consola de Cloud Eye?

En los siguientes escenarios, la tasa de salida supervisada por ELB es incompatible con las estadísticas de uso de ancho de banda de EIP en Cloud Eye:

- Si el tráfico no excede el ancho de banda establecido para la EIP, el ancho de banda no está limitado y Cloud Eye recopila estadísticas en la red pública mientras que ELB recopila datos en la red privada.
- Si el tráfico excede el ancho de banda establecido para la EIP, el ancho de banda es limitado. El tráfico al sistema de ELB pasa con una trayectoria que es diferente de la trayectoria en la que el tráfico pasa a la EIP.

14.2 ¿Cuáles son las diferencias entre los códigos de estado de capa 7 y los códigos de estado backend en las métricas de ELB?

Los oyentes de HTTP o de HTTPS terminan las conexiones de TCP. En otras palabras, hay dos conexiones de TCP entre el cliente y un servidor backend, una entre el cliente y el balanceador de carga, y la otra entre el balanceador de carga y el servidor backend. La comunicación entre el cliente y el servidor backend se divide en dos partes. Después de recibir una solicitud de HTTP, el balanceador de carga analiza la solicitud y enruta la solicitud analizada al servidor backend para su procesamiento. El servidor backend devuelve una respuesta al balanceador de carga después de recibir la solicitud. A continuación, el balanceador de carga analiza la respuesta y devuelve la respuesta analizada al cliente. Por lo tanto, hay dos tipos de códigos de estado: los códigos de estado backend devueltos por el servidor de backend al balanceador de carga y los códigos de estado de Capa 7 devueltos por el balanceador de carga al cliente.

Puede encontrarse con las siguientes situaciones:

- El servidor backend devuelve un código de estado, y el balanceador de carga transmite directamente el código de estado al cliente. En este caso, el código de estado de Capa 7 es el mismo que el código de estado de backend.
- Si la conexión entre el balanceador de carga y el servidor backend es anormal o se agota, el balanceador de carga devuelve HTTP 502 o 504 al cliente.
- Si la configuración de oyente o el formato o contenido de solicitud es incorrecto, el balanceador de carga devuelve directamente un código de estado HTTP 4xx o 502 al cliente, y no encamina la solicitud al servidor backend. En este caso, solo habrá un código de estado de Capa 7, pero no habrá ningún código de estado de backend.

14.3 ¿Por qué hay un gran número de errores de HTTP 499?

Cuando ve el código de estado de HTTP 499, el cliente ha cerrado la conexión mientras el servidor todavía está procesando la solicitud.

Las causas posibles son las siguientes:

- El tiempo de espera de la solicitud puede no ser lo suficientemente largo para que el cliente envíe solicitudes de HTTP antes de que se cierre una conexión. Compruebe el campo **request_time** en el log de acceso para ver el tiempo total de procesamiento de solicitudes y establecer un tiempo de espera de solicitud adecuado.
- Su balanceador de carga puede estar sobrecargado con tráfico, causando pérdida de paquetes debido al límite de ancho de banda. Compruebe el uso del ancho de banda saliente de su balanceador de carga en la consola de Cloud Eye. Para obtener más información, consulte **Métricas de monitoreo**.
- La red que conecta el cliente y el balanceador de carga puede ser inestable, lo que provoca un retraso de ida y vuelta largo o pérdida de paquetes. Compruebe los campos **request_time** y **tcpinfo_rtt** en el log de acceso o los paquetes de captura para comprobar si la red es normal.
- El servidor backend puede tardar más tiempo que el intervalo de tiempo de espera de solicitud para procesar solicitudes. Compruebe si la CPU, la memoria y la red del servidor backend tienen cuellos de botella de rendimiento.
- El cliente cierra la conexión antes de recibir una respuesta del servidor debido a algunas razones desconocidas. Compruebe si el cliente cierra la conexión antes de completar una solicitud de HTTP.

15 Facturación

15.1 ¿Cuándo necesito el ancho de banda público para ELB?

Para acceder a un balanceador de carga a través de Internet, debe comprar una EIP, establecer un ancho de banda para la EIP y vincular la EIP al balanceador de carga. Si accede al balanceador de carga dentro de una VPC, no se requiere EIP ni ancho de banda.

Si accede a los servidores backend con sus EIP, la EIP y el ancho de banda del balanceador de carga no se utilizan.

15.2 ¿Se me facturará tanto el ancho de banda utilizado por el balanceador de carga como el ancho de banda utilizado por los servidores backend?

Esto depende de sus servicios. Si solo se accede a los servidores backend desde una VPC, no es necesario vincular una EIP a cada servidor backend y asignar ancho de banda porque las solicitudes de los clientes son recibidas y enrutadas a los servidores backend por el balanceador de carga. Solo necesita vincular una EIP a cada servidor backend si necesitan proporcionar servicios accesibles desde Internet. En ese caso, debe pagar por el ancho de banda utilizado por su balanceador de carga y también el ancho de banda utilizado por los servidores backend.

15.3 ¿Necesito ajustar el ancho de banda de los balanceadores de carga compartida según el ancho de banda utilizado por los servidores backend?

- Si se utiliza un balanceador de carga de red pública, el ancho de banda utilizado por su EIP depende del tráfico entrante. No está determinado por el ancho de banda utilizado por los servidores backend. Sin embargo, es posible que tenga que ajustar su ancho de banda si hay un aumento en el tráfico entrante, lo que hará que el balanceador de carga se amplíe automáticamente.

- Si el balanceador de carga se utiliza en una red privada, no es necesario ajustarlo.

15.4 ¿Puedo modificar el ancho de banda de un balanceador de carga?

Sí. Para obtener más información, consulte **Modificación del ancho de banda**.

15.5 ¿Qué funciones no estarán disponibles si un balanceador de carga está congelado?

Un balanceador de carga puede congelarse por cualquiera de las siguientes razones:

- Saldo de cuenta insuficiente
- Seguridad pública

Cuando se congela un balanceador de carga dedicado, las siguientes funciones se verán afectadas:

1. El balanceador de carga ya no distribuirá el tráfico entrante.
2. Se detendrá la función de comprobación de estado. Los resultados de la comprobación de estado de los servidores backend que se muestran en la consola son los resultados que se obtuvieron antes de congelar el balanceador de carga.
3. El balanceador de carga dejará de informar los datos de supervisión a Cloud Eye.
4. No se pueden realizar las siguientes operaciones con las invocaciones a la API:
   a. Modificación de los parámetros del balanceador de carga excepto **Name** y **Tag**
   b. Eliminación de un balanceador de carga si está congelado debido a violaciones de las normas de seguridad pública

      En este caso, los recursos asociados con el balanceador de carga, tales como listeners, grupos de servidores backend, servidores backend, comprobaciones de estado, políticas de reenvío y reglas de reenvío, no se pueden crear, eliminar o modificar.

