

nube privada virtual

Preguntas frecuentes

Edición 01
Fecha 2023-04-17



Copyright © Huawei Technologies Co., Ltd. 2023. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos



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

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Índice

1 Preguntas generales.....	1
1.1 ¿Qué es una cuota?.....	1
2 Facturación y Pagos.....	3
2.1 ¿Me cobrarán por utilizar el servicio de VPC?.....	3
2.2 ¿Cómo se factura una EIP?.....	3
2.3 ¿Cómo cambio mi modo de facturación de EIP de pago por uso a anual/mensual?.....	9
2.4 ¿Cómo cambio la opción de facturación de EIP de ancho de banda a tráfico o de tráfico a ancho de banda?.....	10
2.5 ¿Por qué me siguen facturando después de que se hayan eliminado todas las VPC?.....	11
3 VPC y subredes.....	12
3.1 ¿Qué es Virtual Private Cloud?.....	12
3.2 ¿Qué bloques CIDR están disponibles para el servicio de VPC?.....	13
3.3 ¿Cuántas VPC puedo crear?.....	14
3.4 ¿Las subredes pueden comunicarse entre sí?.....	14
3.5 ¿Cuáles bloques CIDR de subred están disponibles?.....	14
3.6 ¿Puedo modificar el bloque CIDR de una subred?.....	14
3.7 ¿Cuántas subredes puedo crear?.....	14
3.8 ¿Cómo hago que el tiempo de arrendamiento DHCP cambiado de una subred surta efecto inmediatamente?.....	15
3.9 ¿Por qué no puedo eliminar mis VPC y subredes?.....	16
3.10 ¿Puedo cambiar la VPC de un ECS?.....	21
3.11 ¿Por qué se pierde la dirección IP de ECS después de cambiar la hora del sistema?.....	21
3.12 ¿Cómo cambio la dirección del servidor de DNS de un ECS?.....	21
4 EIP.....	24
4.1 ¿Cómo asigno o recupero una EIP específica?.....	24
4.2 ¿Cuáles son las diferencias entre EIP, dirección IP privada y dirección IP virtual?.....	24
4.3 ¿Cómo accedo a Internet mediante un enlace de EIP a una NIC de extensión?.....	26
4.4 ¿Cuáles son las diferencias entre las NIC primarias y de extensión de los ECS?.....	27
4.5 ¿Se puede cambiar una EIP que usa ancho de banda dedicado para usar ancho de banda compartido?.....	28
4.6 ¿Puedo vincular una EIP a varios ECS?.....	28
4.7 How Do I Access an ECS with an EIP Bound from the Internet?.....	28
4.8 ¿Qué es la política de asignación de EIP?.....	28
4.9 ¿Puedo vincular una EIP de un ECS a otro ECS?.....	29
4.10 ¿Una EIP cambia con el tiempo?.....	29

4.11 ¿Puedo comprar una específica?.....	29
4.12 ¿Cómo puedo consultar la región de mis EIP?.....	29
4.13 ¿Puede un ancho de banda ser utilizado por varias cuentas?.....	30
4.14 ¿Cómo cambio una EIP para una instancia?.....	30
4.15 ¿Puedo vincular una EIP a un recurso en la nube en otra región?.....	31
4.16 ¿Puedo cambiar la región de mi EIP?.....	31
5 Interconexiones de VPC.....	32
5.1 ¿Cuántas interconexiones de VPC puedo crear en una cuenta?.....	32
5.2 ¿Una interconexión de VPC puede conectar las VPC en diferentes regiones?.....	32
5.3 ¿Por qué falló la comunicación entre las VPC que estaban conectadas por una interconexión de VPC?.....	32
6 Direcciones IP virtuales.....	38
6.1 ¿Por qué no se puede hacer ping a la dirección IP virtual después de vincularla a una NIC de ECS?.....	38
6.2 ¿Cómo puedo vincular una dirección IP virtual en Huawei Cloud a un servidor en un centro de datos local?.....	43
6.3 ¿Por qué la red está desconectada entre los servidores usando una dirección IP virtual después de una conmutación activa/en espera?.....	43
7 Ancho de banda.....	44
7.1 ¿Qué son el ancho de banda entrante y el ancho de banda saliente?.....	44
7.2 ¿Cómo sé si se ha superado el límite de ancho de banda de mi EIP?.....	45
7.3 ¿Cuáles son las diferencias entre el ancho de banda de EIP y el ancho de banda de la red privada?.....	47
7.4 ¿Cuál es el rango de tamaño del ancho de banda?.....	47
7.5 ¿Qué tipos de ancho de banda están disponibles?.....	47
7.6 ¿Cuáles son las diferencias entre un ancho de banda dedicado y un ancho de banda compartido?.....	48
7.7 ¿Cómo puedo comprar un ancho de banda compartido?.....	48
7.8 ¿Hay un límite en el número de las EIP que se pueden agregar a cada ancho de banda compartido?.....	48
7.9 ¿Puedo aumentar mi ancho de banda facturado anualmente/mensualmente y luego disminuirlo?.....	48
7.10 ¿Cuál es la relación entre el ancho de banda y la tasa de carga/descarga?.....	49
7.11 ¿Cuáles son las diferencias entre BGP estático, BGP dinámico y BGP premium?.....	49
8 Conectividad.....	51
8.1 ¿Permite una VPN la comunicación entre dos VPC?.....	51
8.2 ¿Por qué Internet o los nombres de dominio internos en la nube son inaccesibles a través de nombres de dominio cuando mi ECS tiene varias NIC?.....	51
8.3 ¿Cuáles son las prioridades de la ruta personalizada y la EIP si ambas están configuradas para que un ECS permita que el ECS acceda a Internet?.....	52
8.4 ¿Por qué hay interrupciones intermitentes cuando un host local accede a un sitio web construido en un ECS?.....	52
8.5 ¿Por qué los ECS que utilizan las direcciones IP privadas en la misma subred solo admiten la comunicación unidireccional?.....	53
8.6 ¿Por qué falla la comunicación entre dos ECS en la misma VPC o ocurre una pérdida de paquetes cuando se comunican?.....	54
8.7 ¿Por qué mi ECS no puede usar Cloud-init?.....	56
8.8 ¿Por qué mi ECS no puede acceder a Internet incluso después de que una EIP está vinculada?.....	61
8.9 ¿Cómo manejo un fallo de red del IB?.....	64
8.10 ¿Por qué mi ECS no puede comunicarse en una red de nivel 2 o 3?.....	66

8.11 ¿Cómo manejo un fallo de red BMS?.....	68
8.12 ¿Por qué mi ECS no puede obtener una dirección IP?.....	69
8.13 ¿Cómo manejo un fallo de red de conexión directa o VPN?.....	71
8.14 ¿Por qué se puede acceder a mi servidor desde Internet pero no puede acceder a Internet?.....	73
8.15 ¿Por qué no puedo acceder a sitios web por las direcciones IPv6 después de configurar la pila dual IPv4/IPv6?....	75
8.16 ¿Por qué mi ECS no se comunica con los otros después de haber instalado el firewall?.....	77
9 Enrutamiento.....	79
9.1 ¿Cómo configuro las rutas basadas en políticas para un ECS con varias NIC?.....	79
9.2 ¿Una tabla de ruta puede abarcar varias VPC?.....	79
9.3 ¿Cuántas rutas puede contener una tabla de rutas?.....	80
9.4 ¿Existen restricciones en el uso de una tabla de rutas?.....	80
9.5 ¿Se facturará una tabla de ruta?.....	80
9.6 ¿Se aplican las mismas prioridades de enrutamiento a las conexiones de conexión directa y a las rutas personalizadas en la misma VPC?.....	80
9.7 ¿Hay diferentes prioridades de enrutamiento de la VPN y las rutas personalizadas en la misma VPC?.....	80
10 Seguridad.....	81
10.1 ¿Las reglas del grupo de seguridad se consideran iguales si todos los parámetros, excepto su descripción, son iguales?.....	81
10.2 ¿Cuáles son los requisitos para eliminar un grupo de seguridad?.....	81
10.3 ¿Por qué se bloquea el acceso saliente en el puerto TCP 25?.....	82
10.4 ¿Cómo distingo las instancias asociadas a un grupo de seguridad?.....	82
10.5 ¿Puedo cambiar el grupo de seguridad de un ECS?.....	83
10.6 ¿Cuántos grupos de seguridad puedo crear?.....	83
10.7 ¿Se facturará a un grupo de seguridad?.....	83
10.8 ¿Cómo configuro un grupo de seguridad para protocolos multicanal?.....	84
10.9 ¿Cuántas ACL de red puedo crear?.....	84
10.10 Does a Security Group Rule or a ACL de red Rule Immediately Take Effect for Existing Connections After It Is Modified?.....	84
10.11 ¿Por qué algunos puertos son inaccesibles?.....	85
10.12 ¿Por qué todavía se permite el acceso desde una dirección IP específica después de que se haya agregado una regla de ACL de red que niega el acceso desde la dirección IP?.....	85
10.13 ¿Por qué no entran en vigor las reglas de mi grupo de seguridad?.....	86

1 Preguntas generales

1.1 ¿Qué es una cuota?

¿Qué es una cuota?

Una cuota limita la cantidad de un recurso disponible para los usuarios, evitando así picos en el uso del recurso. Por ejemplo, una cuota de VPC limita el número de VPC que se pueden crear.

También puede solicitar un aumento de la cuota si su cuota existente no puede cumplir con sus requisitos de servicio.

¿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 1-1 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 1-2 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**.

2 Facturación y Pagos

2.1 ¿Me cobrarán por utilizar el servicio de VPC?

El servicio de VPC es gratuito, pero la EIP y el ancho de banda utilizado junto con una VPC se facturarán según los precios estándar.

2.2 ¿Cómo se factura una EIP?

EIP se puede facturar de forma anual/mensual o de pago por uso. Las opciones de facturación y los elementos de facturación varían según el modo de facturación.

- [Figura 2-1](#)
- [Tabla 2-1](#)

Figura 2-1 Facturación de EIP

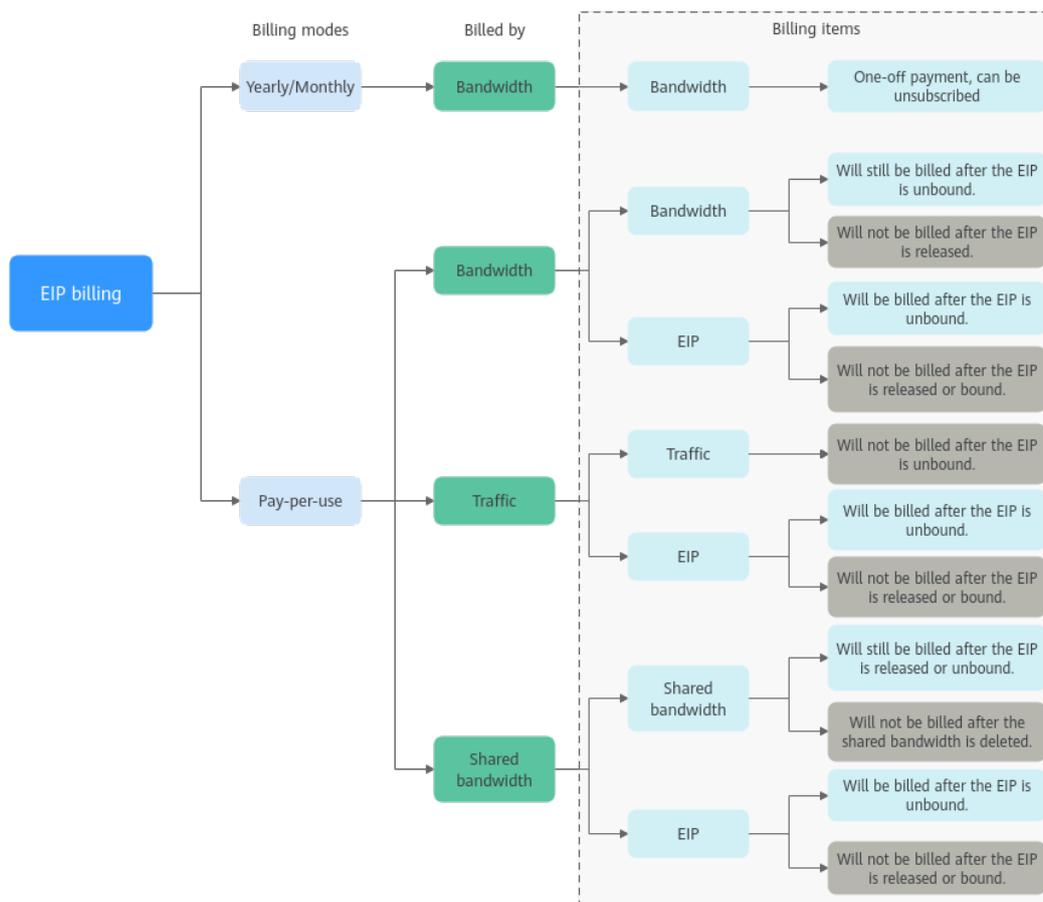


Tabla 2-1 Descripción de facturación de EIP

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
Anual/Mensual	Ancho de banda	Ancho de banda	Si compra un EIP anual/mensual, solo tendrá que pagar por el ancho de banda incluido en la suscripción. Se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en su uso de tráfico.	Puede darse de baja de una suscripción anual/mensual. Su tarifa de uso real y algunas tarifas preferenciales se deducirán del monto del reembolso.

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
Pago por uso	Ancho de banda	<ul style="list-style-type: none"> ● Ancho de banda ● EIP 	<p>Si un EIP de pago por uso se factura por ancho de banda:</p> <ul style="list-style-type: none"> ● Tarifa de ancho de banda: se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en el uso del tráfico. Después de comprar el EIP, puede cambiar el tamaño de ancho de banda especificado. El ancho de banda que utilice no excederá el ancho de banda especificado. ● Tarifa de retención de EIP: la EIP se facturará si no está vinculada a ninguna instancia y no se libera. 	<p>Después de comprar un EIP:</p> <ul style="list-style-type: none"> ● Si el EIP no está vinculado a ninguna instancia, se facturará tanto el EIP como su ancho de banda. ● Si el EIP está vinculado a una instancia, solo se facturará el ancho de banda. El ancho de banda se facturará sin importar si la instancia vinculada al EIP se está ejecutando o no. ● Después de que el EIP se desvincule de una instancia, se seguirá facturando el ancho de banda. A menos que se publique, el EIP también se facturará. ● Si se libera el EIP, tanto el EIP como su ancho de banda no se facturarán.

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
	Tráfico	<ul style="list-style-type: none"> ● Tráfico ● EIP 	<p>Si un EIP de pago por uso es facturado por tráfico:</p> <ul style="list-style-type: none"> ● Tarifa de tráfico: se le factura en función de su tipo de EIP y el tráfico total utilizado que sale de la nube. El tamaño de ancho de banda que establezca solo se utiliza para limitar la velocidad máxima de transferencia de datos. Para evitar altas tarifas causadas por el tráfico de ráfagas, especifique un tamaño de ancho de banda adecuado cuando compre un EIP. ● Tarifa de retención de EIP: la EIP se facturará si no está vinculada a ninguna instancia y no se libera. 	<p>Después de comprar un EIP:</p> <ul style="list-style-type: none"> ● Si el EIP no está vinculado a ninguna instancia, solo se facturará al EIP. ● Si el EIP está vinculado a una instancia, solo se facturará el tráfico utilizado. Si la instancia vinculada al EIP deja de funcionar y no se genera tráfico, no habrá tráfico ni tarifas de EIP. ● Después de que el EIP se desvincule de una instancia, el tráfico no se facturará, pero el EIP se facturará. ● Si se libera el EIP, el EIP no se facturará.

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
	Anchos de banda compartidos	<ul style="list-style-type: none"> ● Anchos de banda compartidos ● EIP 	<p>Si se agrega un EIP de pago por uso a un ancho de banda compartido:</p> <ul style="list-style-type: none"> ● Tarifa de ancho de banda compartido: Solo se facturará el ancho de banda compartido. No habrá costes adicionales de ancho de banda o tráfico para los EIP añadidos al ancho de banda compartido. ● Tarifa de retención de EIP: la EIP se facturará si no está vinculada a ninguna instancia y no se libera. 	<p>Después de comprar un EIP:</p> <ul style="list-style-type: none"> ● Anchos de banda compartidos <ul style="list-style-type: none"> - Cualquier operación en el EIP no afecta a la facturación del ancho de banda compartido. Por ejemplo, si ha liberado el EIP pero no ha eliminado el ancho de banda compartido, el ancho de banda compartido todavía se facturará. - Después de eliminar un ancho de banda compartido, ya no se facturará. ● EIP <ul style="list-style-type: none"> - Si el EIP no está vinculado a ninguna instancia, se facturará al EIP. - Si el EIP no está vinculado de una instancia, se facturará al EIP para mantenerlo asignado a su cuenta a menos que se libere. - Si el EIP se libera o se vincula a una instancia, el EIP no se facturará.

Puede agregar varios EIP en la misma región a un ancho de banda compartido para reducir los costos. Un ancho de banda compartido se puede facturar anual/mensual o de pago por uso.

Para obtener más información, consulte [Tabla 2-2](#). Actualmente, solo se pueden agregar EIP de pago por uso a un ancho de banda compartido.

- Puede agregar un EIP a un ancho de banda compartido al comprar el EIP.
- También puede agregar un EIP existente a un ancho de banda compartido. Después de agregar el EIP a un ancho de banda compartido, no habrá ancho de banda adicional ni costes de tráfico, y solo se facturará el ancho de banda compartido.

Tabla 2-2 Detalles de facturación de ancho de banda compartido

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación
Anual/ Mensual	Ancho de banda	Ancho de banda	Si compra un ancho de banda compartido anual/mensual, se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en el uso del tráfico.
Pago por uso	Ancho de banda	Ancho de banda	Se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en el uso del tráfico. Después de comprar un ancho de banda compartido, puede cambiar el tamaño de ancho de banda especificado. El ancho de banda que utilice no excederá el ancho de banda especificado.

Consulte la sección [Facturación](#).

2.3 ¿Cómo cambio mi modo de facturación de EIP de pago por uso a anual/mensual?

Tabla 2-3 Billing mode change description

Change	Description
From yearly/monthly to pay-per-use	<ul style="list-style-type: none"> ● An EIP billed on a yearly/monthly basis can be directly changed to be billed by bandwidth on a pay-per-use basis. ● An EIP billed on a yearly/monthly basis cannot be directly changed to be billed by traffic on a pay-per-use basis. To change this: <ol style="list-style-type: none"> 1. First, change the EIP billed on a yearly/monthly basis to be billed by bandwidth on a pay-per-use basis. 2. Then, change the EIP billed by bandwidth on a pay-per-use basis to be billed by traffic on a pay-per-use basis. <p>The new billing mode takes effect only after the yearly/monthly billing expires.</p>
From pay-per-use to yearly/monthly	<ul style="list-style-type: none"> ● An EIP that is billed by bandwidth on a pay-per-use basis can be directly changed to be billed on a yearly/monthly basis. ● An EIP that is billed by traffic on a pay-per-use basis cannot be directly changed to be billed on a yearly/monthly basis. To change this: <ol style="list-style-type: none"> 1. First, change the EIP billed by traffic on a pay-per-use basis to be billed by bandwidth on a pay-per-use basis. 2. Then, change the EIP billed by bandwidth on a pay-per-use basis to be billed on a yearly/monthly basis. <p>After the change is successful, the new billing mode takes effect immediately.</p>

De anual/mensual a pago por uso

1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la página, elija **Billing & Costs > Renewal**.
3. En la lista de recursos, busque el EIP cuyo modo de facturación necesita cambiarse.
4. Busque la fila que contiene el EIP y elija **More > Change to Pay-per-Use After Expiration** en la columna **Operation**.
5. Confirme la configuración y haga clic en **Change to Pay-per-Use**.

Una vez completada la operación, se cambia el EIP anual/mensual para facturarse por ancho de banda sobre una base de pago por uso.

De pago por uso a anual/mensual

1. Inicie sesión en la consola de gestión.
2. En **Networking**, haga clic en **Elastic IP**.
3. En la lista de EIP, cambie el modo de facturación de un único EIP o de varios EIP facturados por ancho de banda de pago por uso a anual/mensual.
 - Único EIP:
Busque la fila que contiene el EIP y haga clic en **Change Billing Mode** en la columna **Operation**.
 - Múltiples EIP:
Seleccione EIPs y haga clic en **Change Billing Mode** en la esquina superior izquierda de la lista EIP.
4. En el cuadro de diálogo mostrado, confirme la información y haga clic en **Yes**.
5. En la página **Change Subscriptions**, establezca parámetros como **Renewal Duration**.
6. Haga clic en **Pay**.

2.4 ¿Cómo cambio la opción de facturación de EIP de ancho de banda a tráfico o de tráfico a ancho de banda?

NOTA

- El cambio del modo de facturación no modifica las EIP ni interrumpe su uso.
- Los siguientes escenarios de cambio solo se aplican a las EIP de pago por uso.
- Las EIP anuales/mensuales facturadas por ancho de banda no se pueden cambiar directamente a las EIP de pago por uso facturadas por tráfico.

Tabla 2-4 Descripción del cambio

Cambio	Descripción
Desde la facturación por tráfico (pago por uso) hasta la facturación por ancho de banda (pago por uso)	Una EIP facturado por tráfico sobre una base de pago por uso puede cambiarse directamente para ser facturado por ancho de banda sobre una base de pago por uso. Una vez que se realiza el cambio, el nuevo modo de facturación se aplica inmediatamente.
Desde la facturación por ancho de banda (pago por uso) hasta la facturación por tráfico (pago por uso)	Una EIP facturado por ancho de banda sobre una base de pago por uso puede cambiarse directamente para ser facturado por tráfico sobre una base de pago por uso. Una vez que se realiza el cambio, el nuevo modo de facturación se aplica inmediatamente.

De facturación por tráfico a por ancho de banda (EIP de pago por uso)

1. Inicie sesión en la consola de gestión.
2. En **Networking**, haga clic en **Elastic IP**.
3. En la lista EIP, busque la fila que contiene el EIP, haga clic en **More** en la columna **Operation** y haga clic en **Modify Bandwidth**.
4. En la página **Modify Bandwidth**, cambie la opción de facturación según se le indique. También puede cambiar el nombre y el tamaño del ancho de banda.
5. Haga clic en **Next**.
6. En la página mostrada, confirme las configuraciones y haga clic en **Submit**.

2.5 ¿Por qué me siguen facturando después de que se hayan eliminado todas las VPC?

Symptom

Charges are generated even all VPCs have been deleted.

Possible Causes

VPCs are free, but you are still billed for the EIPs and public bandwidth used together with a VPC.

- EIPs that use public bandwidth may be in use in other projects or regions. You can view all EIPs in the billing center, locate the EIP, and switch to the project or region where the EIP is located and delete it.
- The information in the bill is from your previous settlement period. Generally, fees are not deducted from your account immediately after pay-per-use EIPs are released. Instead, bills are generated and fees are deducted from your account only after the settlement period ends.

3 VPC y subredes

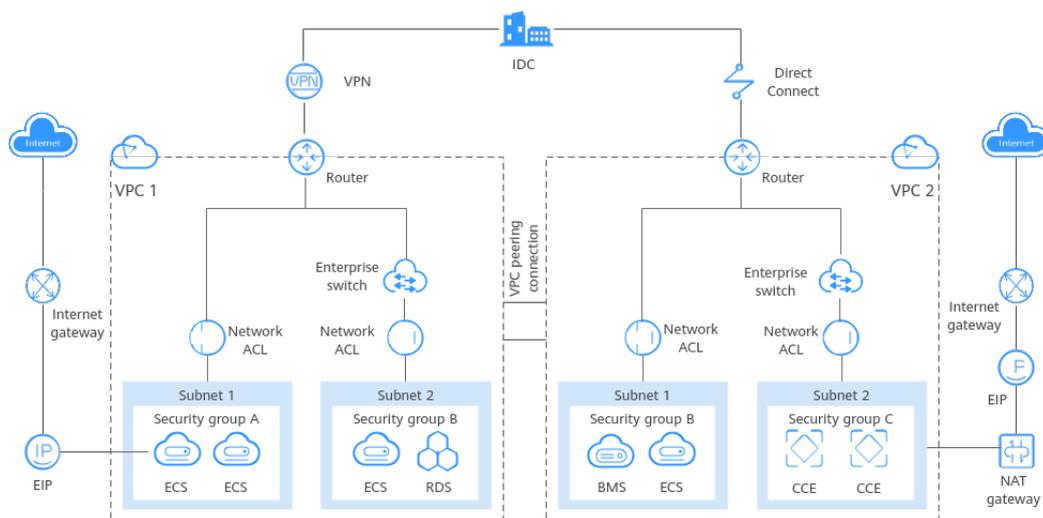
3.1 ¿Qué es Virtual Private Cloud?

El servicio Virtual Private Cloud (VPC) le permite aprovisionar las redes virtuales aisladas y privadas lógicamente para recursos en la nube, como servidores en la nube, contenedores y bases de datos. Puede personalizar subredes, grupos de seguridad, ACL de red y asignar EIP y anchos de banda. Con Direct Connect o Virtual Private Network (VPN), puede conectar sus VPC a un centro de datos local.

Arquitectura del producto

La arquitectura del producto consta de componentes de VPC, características de seguridad y opciones de conectividad de VPC.

Figura 3-1 Arquitectura



Componentes de VPC

Cada VPC consta de un bloque CIDR privado, tablas de ruta y al menos una subred.

- **Bloque de CIDR privado:** Al crear una VPC, debe especificar el bloque de CIDR privado utilizado por la VPC. El servicio de VPC admite los siguientes bloques CIDR: 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, y 192.168.0.0 - 192.168.255.255
- **Subred:** Los recursos de la nube, como servidores y bases de datos en la nube, deben implementarse en las subredes. Después de crear una VPC, divida la VPC en una o más subredes. Cada subred debe estar dentro de la VPC.
- **Tabla de rutas:** Cuando se crea una VPC, el sistema genera automáticamente una tabla de rutas predeterminada. La tabla de rutas garantiza que todas las subredes de la VPC puedan comunicarse entre sí. Si las rutas de la tabla de rutas predeterminada no pueden cumplir los requisitos de la aplicación, (por ejemplo, un ECS sin una dirección IP elástica (EIP) vinculada necesita acceder a Internet), puede crear una tabla de ruta personalizada.

Características de seguridad

Los grupos de seguridad y las ACL de red garantizan la seguridad de los recursos de nube implementados en una VPC. Un grupo de seguridad actúa como un firewall virtual para proporcionar reglas de acceso para instancias que tienen los mismos requisitos de seguridad y son de confianza mutua en una VPC. Una ACL de red se puede asociar a subredes que tienen los mismos requisitos de control de acceso. Puede agregar las reglas entrantes y las salientes para controlar con precisión el tráfico entrante y e saliente en el nivel de subred.

Conectividad de VPC

Huawei Cloud ofrece múltiples opciones de conectividad de VPC para satisfacer diversos requisitos.

- La interconexión de VPC permite que dos VPC de la misma región se comuniquen entre sí mediante direcciones IP privadas.
- Elastic IP o NAT Gateway permite que los ECS en una VPC se comuniquen con Internet.
- La red privada virtual (VPN), Cloud Connect o Direct Connect pueden conectar una VPC a su centro de datos.

3.2 ¿Qué bloques CIDR están disponibles para el servicio de VPC?

En la siguiente tabla se enumeran los bloques CIDR privados que se pueden especificar al crear una VPC. Tenga en cuenta lo siguiente al seleccionar un bloque CIDR de VPC:

- **Número de direcciones IP:** reserve suficientes direcciones IP en caso de crecimiento del negocio.
- **Intervalo de direcciones IP:** Evite conflictos de direcciones IP si necesita conectar una VPC a un centro de datos local o conectar dos VPC.

El servicio de VPC admite los siguientes bloques CIDR:

Bloque CIDR de VPC	Rango de direcciones IP	Número máximo de direcciones IP
10.0.0.0/8-24	10.0.0.0-10.255.255.255	$2^{24}-2=16777214$
172.16.0.0/12-24	172.16.0.0-172.31.255.255	$2^{20}-2=1048574$

Bloque CIDR de VPC	Rango de direcciones IP	Número máximo de direcciones IP
192.168.0.0/16-24	192.168.0.0-192.168.255.255 5	$2^{16-2}=65534$

3.3 ¿Cuántas VPC puedo crear?

De forma predeterminada, puede crear un máximo de cinco VPC en su cuenta. Si el número de VPC no puede cumplir con sus requisitos de servicio, [envíe un ticket de servicio](#).

3.4 ¿Las subredes pueden comunicarse entre sí?

Las subredes de la misma VPC pueden comunicarse entre sí, pero las subredes de diferentes VPC no pueden comunicarse entre sí de forma predeterminada. No obstante, puede crear conexiones del mismo nivel de VPC para permitir que las subredes que están en distintas VPC se comuniquen entre sí.

NOTA

Si las subredes tienen las ACL de red asociadas, las reglas de ACL de red deben permitir la comunicación entre las subredes.

3.5 ¿Cuáles bloques CIDR de subred están disponibles?

Se debe incluir un bloque CIDR de subred en su bloque CIDR de VPC. Los bloques de CIDR de VPC soportados son **10.0.0.0/8 - 24**, **172.16.0.0/12 - 24**, y **192.168.0.0/16 - 24**. El tamaño de bloque permitido de una subred está entre la máscara de red de su bloque CIDR de VPC y la máscara de red /28.

3.6 ¿Puedo modificar el bloque CIDR de una subred?

Puede modificar el bloque CIDR de una subred sólo cuando está creando la subred. Después de crear la subred, no puede modificar su bloque CIDR.

3.7 ¿Cuántas subredes puedo crear?

De forma predeterminada, puede crear un máximo de 100 subredes en su cuenta en la nube. Si el número de subredes no puede cumplir sus requisitos de servicio, [envíe un ticket de servicio](#) para solicitar un aumento de cuota.

3.8 ¿Cómo hago que el tiempo de arrendamiento DHCP cambiado de una subred surta efecto inmediatamente?

Escenarios

Después de cambiar el tiempo de concesión DHCP en la consola, los ECS existentes no utilizarán la nueva concesión DHCP hasta que sea necesario renovar la concesión actual. Una liberación se renueva cuando ha transcurrido la mitad del tiempo de arrendamiento. Por ejemplo, si el contrato de arrendamiento de 30 días establecido el 1 de enero, el contrato de arrendamiento se renovará el 15 de enero.

Si necesita hacer que el nuevo tiempo de concesión DHCP surta efecto inmediatamente para los ECS en la subred, consulte el procedimiento siguiente.

NOTA

Si renueva la concesión DHCP manualmente, se liberarán las direcciones IP actuales de los ECS. Los ECS no tienen direcciones IP hasta que la nueva versión surta efecto y se les asignan nuevas direcciones IP, lo que puede causar la interrupción del servicio.

También puede reiniciar directamente los ECS para que la nueva versión DHCP surta efecto inmediatamente.

Procedimiento

Para un ECS de Windows:

1. Después de cambiar el tiempo de concesión DHCP en la consola, inicie sesión en el ECS cuya concesión desea renovar.
2. Elija **Start > Run**. Escriba cmd para abrir la GUI de la operación de DOS.
3. Ejecute el comando **ipconfig /all** para ver el tiempo de caducidad de la concesión DHCP actual.
4. Ejecute el comando **ipconfig /release && ipconfig /renew** para renovar el contrato de arrendamiento. Ejecute de nuevo el comando **ipconfig /all** para ver el resultado.

Para un ECS de Linux:

1. Después de cambiar el tiempo de concesión DHCP en la consola, inicie sesión en el ECS cuya concesión desea renovar.
2. Ejecute el comando **ps -ef | grep dhclient** para comprobar si el cliente que proporciona el servicio DHCP es **dhclient**. Si existe el proceso de la siguiente figura, el cliente es **dhclient**. El archivo de arrendamiento cuya ruta de acceso está junto al parámetro **-lf** contiene la información de arrendamiento. Si el proceso **dhclient** no existe, este procedimiento puede no ser aplicable. En este caso, debe buscar los comandos de operación del cliente DHCP correspondiente.



```
root@vpc8-subnet0-az0-pod0-xen ~# ps -ef | grep dhclient
root      597   537   0 Jun14 ?        00:00:00 /usr/sbin/dhclient -d -q -sf /usr/libexec/mn-dhcp-helper -pf /var/run/dhclient-eth8.pid -lf /var/lib/NetworkManager/dhclient-5f866d0-8bb0-7f7b-45c1-d6ed465f3e83-eth8.lease -cf /var/lib/NetworkManager/dhclient-eth8.conf eth8
```

3. Ejecute el comando **dhclient -r** para liberar la dirección IP actual.
4. Ejecute el comando **killall dhclient && systemctl restart NetworkManager** para obtener la nueva concesión DHCP. Vea el archivo de arrendamiento mencionado en el

paso anterior. Puede ver la última concesión DHCP. El archivo de arrendamiento también contiene la información histórica de arrendamiento. La última información de arrendamiento en el archivo es el último arrendamiento.

```

[root@pc8-subnet0-a2d-pod0-xen ~]# cat /var/lib/NetworkManager/dhclient-5f86b48-8bb8-7ffb-45f1-46edd65f3e83-eth0.lease
lease {
  interface "eth0";
  fixed-address 10.1.1.124;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 864000;
  option routers 10.1.1.1;
  option dhcp-message-type 5;
  option dhcp-server-identifier 10.1.1.254;
  option domain-name-servers 10.1.1.254;
  option interface-mtu 1500;
  option dhcp-renewal-time 432000;
  option dhcp-rebinding-time 756000;
  option broadcast-address 10.1.1.255;
  option rfc3442-classless-static-routes 0,10.1.1.1,32,169,254,169,254,10.1.1,254;
  option host-name "host-10-1-1-124";
  renew 2 2019/06/10 14:09:18;
  rebind 0 2019/06/23 01:53:27;
  expire 1 2019/06/24 07:53:27;
}
lease {
  interface "eth0";
  fixed-address 10.1.1.124;
  option subnet-mask 255.255.255.0;
  option routers 10.1.1.1;
  option dhcp-lease-time 429467295;
  option dhcp-message-type 5;
  option domain-name-servers 10.1.1.254;
  option dhcp-server-identifier 10.1.1.254;
  option interface-mtu 1500;
  option rfc3442-classless-static-routes 0,10.1.1.1,32,169,254,169,254,10.1.1,254;
  option broadcast-address 10.1.1.255;
  option host-name "host-10-1-1-124";
  renew 3 2007/07/02 11:32:40;
  rebind 3 2130/07/16 19:58:09;
  expire 1 2155/07/21 14:46:47;
}

```

3.9 ¿Por qué no puedo eliminar mis VPC y subredes?

Si otros recursos utilizan las VPC y subredes, primero debe eliminar estos recursos según los avisos de la consola antes de eliminar las VPC y subredes. A continuación se proporcionan las instrucciones de eliminación detalladas y la guía de eliminación correspondiente.

- [Supresión de subredes](#)
- [Eliminación de las VPC](#)

AVISO

Las VPC y subredes son gratuitas.

Supresión de subredes

Puede hacer referencia a [Tabla 3-1](#) para eliminar subredes.

Tabla 3-1 Supresión de subredes

Avisos	Motivo
You do not have permission to perform this operation.	Su cuenta no tiene permisos para eliminar subredes.

Avisos	Motivo
Elimine las rutas personalizadas de la tabla de ruta asociada de la subred y luego eliminar la subred.	La tabla de ruta tiene las rutas personalizadas con lo siguiente como el siguiente tipo de salto: <ul style="list-style-type: none"> ● Servidor ● NIC de extensión ● Dirección IP virtual ● Gateway de NAT
Release any virtual IP addresses configured in the subnet and then delete the subnet.	La subred tiene direcciones IP virtuales configuradas.
Release any private IP addresses configured in the subnet and then delete the subnet.	La subred tiene direcciones IP virtuales que no son utilizadas por ninguna instancia.
Delete the resource (ECS or load balancer) that is using the subnet and then delete the subnet.	La subred está siendo utilizada por un ECS o un balanceador de carga.
Delete the load balancer that is using the subnet and then delete the subnet.	La subred está siendo utilizada por un balanceador de carga.
Delete the NAT gateway that is using the subnet and then delete the subnet.	La subred está siendo utilizada por un gateway de NAT.
Delete the resource that is using the subnet and then delete the subnet.	La subred está siendo utilizada por los recursos de la nube.

Eliminación de las VPC

Antes de eliminar una VPC, asegúrese de que se han eliminado todas las subredes de la VPC. Puede hacer referencia a [Tabla 3-2](#) para eliminar VPC.

Tabla 3-2 Eliminación de las VPC

Avisos	Motivo	Solución
You do not have permission to perform this operation.	Su cuenta no tiene permisos para eliminar las VPC.	Póngase en contacto con el administrador de la cuenta para conceder permisos a su cuenta y, a continuación, elimine la VPC. Gestión de permisos
Delete the VPC endpoint	La tabla de ruta de VPC tiene las rutas personalizadas.	Elimine las rutas personalizadas y, a continuación, elimine la VPC.

Avisos	Motivo	Solución
service or the route configured for the service from the VPC route table and then delete the VPC.	La VPC está siendo utilizada por un servicio de punto de conexión de VPC.	Busque el servicio de punto de conexión de VPC en la consola de servicio de punto de conexión de VPC y elimínelo. Eliminación de un servicio de punto de conexión de VPC
This VPC cannot be deleted because it has associated resources.	La VPC está siendo utilizada por los siguientes recursos: <ul style="list-style-type: none"> ● Subred ● Interconexión de VPC ● Tabla de rutas personalizada 	Haga clic en el hipervínculo de nombre de recurso según se le solicite para eliminar el recurso. <ul style="list-style-type: none"> ● Tabla 3-1 ● Eliminación de una interconexión de VPC ● Eliminación de una tabla de ruta
Delete the virtual gateway that is using the VPC and then delete the VPC.	La VPC está siendo utilizada por un gateway virtual de Direct Connect.	En la consola de Direct Connect, localice el gateway virtual y elimínelo. Eliminación de un gateway virtual
Delete the VPN gateway that is using the VPC and then delete the VPC.	La VPC está siendo utilizada por un gateway de VPN.	En la consola de VPN, localice el gateway de VPN y elimínelo. Eliminación de un gateway de VPN
Remove the VPC from the cloud connection and then delete the VPC.	La VPC está siendo utilizada por una conexión de Cloud Connect.	En la consola de Cloud Connect, localice la conexión y elimine la VPC de ella. Eliminación de una instancia de red

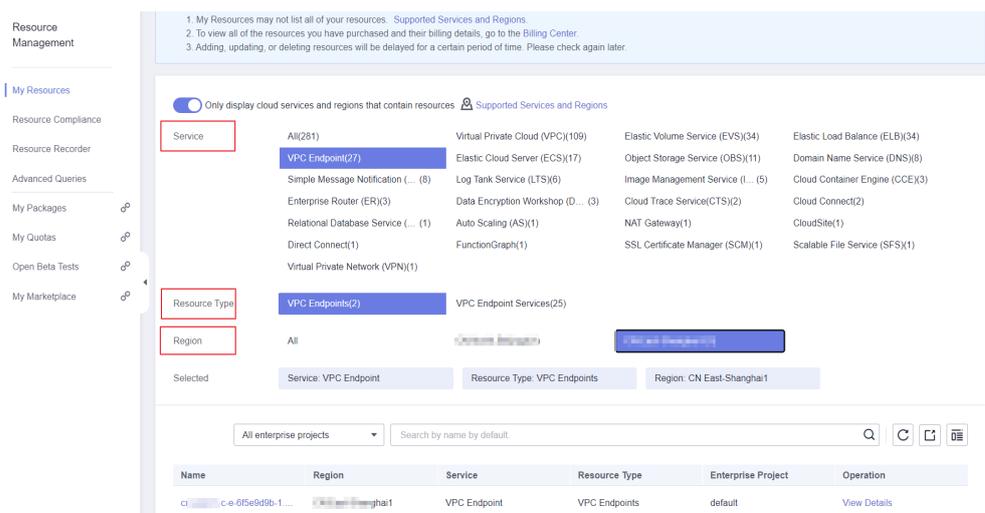
Avisos	Motivo	Solución
Delete all custom security groups in this region and then delete this last VPC.	En la región actual, esta es la última VPC y hay unos grupos de seguridad personalizados. AVISO Solo tiene que eliminar los grupos de seguridad personalizados. El grupo de seguridad predeterminado no afecta a la eliminación de las VPC.	Elimine todos los grupos de seguridad personalizados y, a continuación, elimine la VPC. Eliminación de un grupo de seguridad
Release all EIPs in this region and then delete this last VPC.	En la región actual, esta es la última VPC y hay unas EIP.	Libere todas las EIP y luego elimine la VPC. Liberación de una EIP

Búsqueda de recursos en la nube

1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la consola, seleccione **More > Resources > My Resources**.

Se muestra la página **My Resources**.

Figura 3-2 Mis recursos



3. En la página **My Resources**, establezca criterios de búsqueda para encontrar rápidamente los recursos de la subred.
 - **Service:** seleccione un servicio que tenga recursos en subredes.

Tabla 3-3 enumera algunos recursos comunes. Si tiene otros recursos, compruébelos.

- **Resource Type:** Verifique los tipos de recursos.
- **Region:** seleccione la región donde se encuentran la VPC y la subred para filtrar los recursos de la misma región. Las VPC y las subredes solo pueden ser utilizadas por los recursos de su misma región.

Tabla 3-3 Recursos comunes en subredes

Categoría del producto	Servicio
Cómputo	Elastic Cloud Server (ECS)
	Bare Metal Server (BMS)
	Cloud Container Engine (CCE)
	Cloud Container Instance (CCI)
Contenedores	Application Service Mesh (ASM)
Redes	Elastic Load Balance (ELB)
	NAT Gateway
	VPC Endpoint (VPCEP)
Bases de datos	GaussDB
	Relational Database Service (RDS)
	Document Database Service (DDS)
	GaussDB NoSQL
	Distributed Database Middleware (DDM)
Middleware	Distributed Cache Service (DCS) <ul style="list-style-type: none"> ● Instancia de Redis ● instancia de Memcached
	Distributed Message Service (DMS) <ul style="list-style-type: none"> ● Instancia de Kafka ● Instancia de RabbitMQ
EI	MapReduce Service (MRS)
	Data Warehouse Service (DWS)
	Cloud Search Service (CSS)

Si no puede eliminar una subred incluso después de eliminar todos los recursos que contiene, [envíe un ticket de servicio](#).

3.10 ¿Puedo cambiar la VPC de un ECS?

Sí.

Puede hacer clic en **Change VPC** en la columna **Operation** de la página **Elastic Cloud Server**.

Para obtener más información, consulte [Cambio de una VPC](#).

3.11 ¿Por qué se pierde la dirección IP de ECS después de cambiar la hora del sistema?

Causa: esto se produce porque la diferencia de tiempo entre la hora antigua y la nueva es más larga que la hora de concesión DHCP. El tiempo de concesión DHCP predeterminado establecido al crear una subred es de 365 días. Si cambia manualmente la hora del sistema ECS y la diferencia de tiempo entre la hora antigua y la nueva es superior a 365 horas, la concesión DHCP no se puede renovar y se perderá la dirección IP de ECS.

Solución: si necesita cambiar la hora del sistema ECS y la diferencia de tiempo es mayor que la hora de liberación DHCP, cambie el modo de asignación de dirección IP ECS a estático antes de cambiar la hora del sistema ECS.

3.12 ¿Cómo cambio la dirección del servidor de DNS de un ECS?

Escenarios

Esta sección describe cómo cambiar la dirección del servidor DNS de un ECS y hacer que la nueva dirección del servidor DNS surta efecto inmediatamente en el ECS.

Fondo

Los ECS utilizan servidores de DNS privados para la resolución de nombres de dominio en las VPC. Los servidores DNS privados no afectan a la resolución de nombres de dominio para que los ECS accedan a Internet. Además, puede utilizar los servidores de DNS privados para acceder directamente a las direcciones IP privadas de los servicios en la nube, como OBS y SMN. En comparación con el acceso a través de Internet, este acceso cuenta con alto rendimiento y baja latencia.

Antes de que los nombres de dominio privados estén disponibles, las subredes de VPC utilizan el servidor DNS público (114.114.114.114). Para permitir que los ECS de estas VPC accedan a nombres de dominio privados, puede cambiar el servidor de DNS público a los servidores DNS privados configurados para las subredes de VPC. Para obtener instrucciones sobre cómo obtener una dirección de servidor DNS privado, consulte [¿Cuáles son los servidores DNS privados proporcionados por el servicio DNS en Huawei Cloud?](#)

Cambio de servidores de DNS para ECS

Después de cambiar las direcciones de servidor DNS de una subred de VPC, las direcciones de servidor DNS de los ECS en la subred no tendrán efecto inmediatamente.

Para que las direcciones del servidor DNS surtan efecto inmediatamente, haga lo siguiente:

- Reinicie el SO. El ECS obtendrá entonces las nuevas direcciones del servidor DNS del servidor DHCP.

AVISO

El reinicio del SO interrumpirá los servicios en el ECS. Realice esta operación durante las horas de menor actividad.

Como alternativa, espere a que expire la concesión DHCP, que es de 365 días de forma predeterminada. Después de que expire el tiempo de concesión, el servidor de DHCP asigna otra dirección IP y actualiza las direcciones del servidor DNS al ECS.

- Obtenga las nuevas direcciones de servidor DNS.
 - a. Inicie sesión en el ECS.
 - b. Ejecute el siguiente comando para ver la dirección del servidor de DNS del ECS:

```
cat /etc/resolv.conf
```

Si se muestra información similar a la siguiente, 114.114.114.114 es la dirección del servidor DNS del ECS.

```
[root@ecs ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search openstacklocal
nameserver 114.114.114.114
options timeout:1 single-request-reopen
```

- c. Ejecute el siguiente comando para comprobar si el proceso **dhclient** existe:

```
ps -ef | grep dhclient | grep -v grep
```

Si se muestra información similar a la siguiente, no existe ningún proceso (se usa CentOS 8.1 como ejemplo).

En este caso, ejecute el comando **dhclient** para iniciar el proceso y comprobar si el proceso **dhclient** existe.

```
[root@ecs ~]# ps -ef | grep dhclient | grep -v grep
[root@ecs ~]# dhclient
[root@ecs ~]# ps -ef | grep dhclient | grep -v grep
root      5712      1  0 09:52 ?        00:00:00 dhclient
```

Si se muestra información similar a la siguiente, el proceso existe (se usa CentOS 7.2 como ejemplo).

```
[root@ecs ~]# ps -ef | grep dhclient | grep -v grep
root      651  477  0 18:36 ?        00:00:00 /sbin/dhclient -d -q -sf /usr/libexec/um-dhcp-helper -pf /var/run/dhclient-eth0.pid -lf /var/lib/NetworkManager/dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-eth0.lease -cf /var/lib/NetworkManager/dhclient-eth0.conf eth0
```

- d. Ejecute el siguiente comando para liberar la dirección actual del servidor DNS:

```
dhclient -r
```

- e. Ejecute el siguiente comando para reiniciar el proceso **dhclient** y obtener nuevas direcciones de servidor DNS:

```
dhclient
```

- f. Ejecute el siguiente comando para ver las nuevas direcciones de servidor DNS del ECS:

cat /etc/resolv.conf

Si se muestra información similar a la siguiente, 100.125.1.250 y 100.125.64.250 son las nuevas direcciones de servidor DNS del ECS.

```
[root@ecs-...-01 ~]# dhclient -r
[root@ecs-...-01 ~]# dhclient
[root@ecs-...-01 ~]# cat /etc/resolv.conf
options timeout:1 single-request-reopen
; generated by /usr/sbin/dhclient-script
search openstacklocal
nameserver 100.125.1.250
nameserver 100.125.64.250
```

4 EIP

4.1 ¿Cómo asigno o recupero una EIP específica?

Si desea recuperar una EIP que ha liberado o asignar una EIP específico, puede usar API estableciendo el valor de **ip_address** al que desea asignar.

NOTA

- Si el EIP ha sido asignado a otro usuario, no podrá asignar el EIP requerido.
- No se puede utilizar la consola de gestión para asignar una EIP específica.

4.2 ¿Cuáles son las diferencias entre EIP, dirección IP privada y dirección IP virtual?

Los tipos diferentes de direcciones IP tienen las funciones diferentes.

Figura 4-1 Arquitectura de direcciones IP

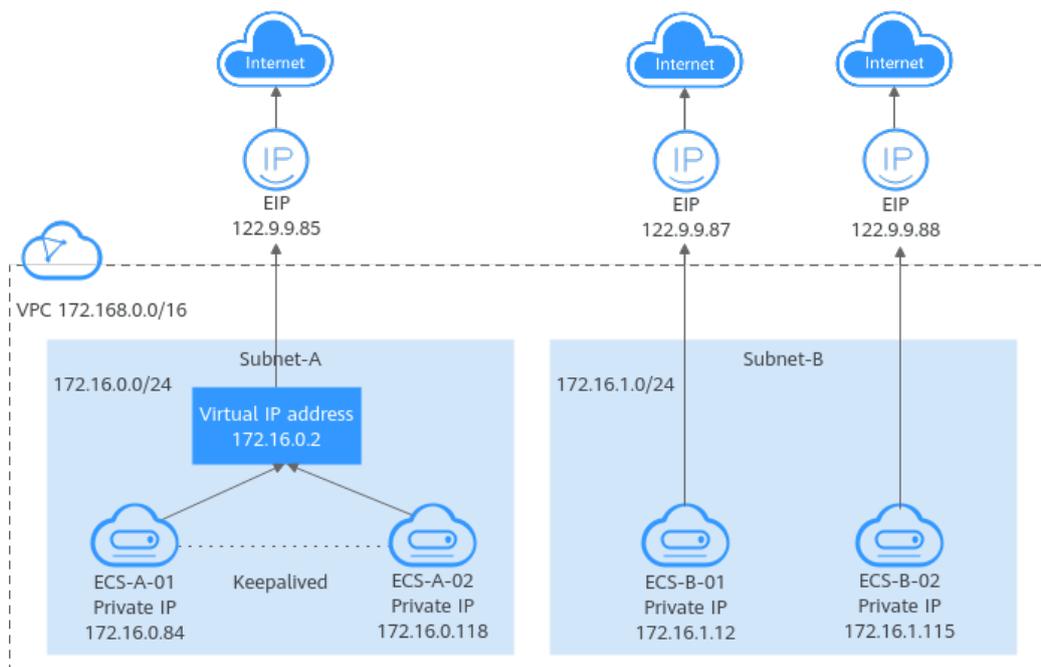


Tabla 4-1 Funciones de diferentes tipos de direcciones IP

Tipo de dirección IP	Descripción	Valor de ejemplo
Dirección IP privada	Las direcciones IP privadas vienen con sus ECS y pertenecen a las subredes de VPC de los ECS. Se utilizan para la comunicación privada en la nube.	<ul style="list-style-type: none"> ● Private IP address of ECS-A-01: 172.16.0.84 ● Private IP address of ECS-B-01: 172.16.1.12
Dirección IP virtual	<p>Una dirección IP virtual se puede compartir entre múltiples ECS. Dos ECS pueden funcionar como un par activo y en espera para lograr una alta disponibilidad mediante el uso de una dirección IP virtual y Keepalived. Si el ECS activo es defectuoso, la dirección IP virtual puede conmutarse dinámicamente al ECS en espera para continuar proporcionando servicios.</p> <p>Para obtener más información acerca de las direcciones IP virtuales, consulte la Descripción de la dirección IP virtual. Para obtener más información acerca de cómo configurar un clúster de alta disponibilidad, consulte la Creación de clústeres de servidores web de alta disponibilidad con Keepalived.</p>	Bind virtual IP address (172.16.0.2) both ECS-A-01 and ECS-A-02. The active/standby switchover of ECS-A-01 and ECS-A-02 can be implemented by using Keepalived.

Tipo de dirección IP	Descripción	Valor de ejemplo
EIP	<p>Los recursos en la nube pueden utilizar EIP para el acceso a Internet.</p> <ul style="list-style-type: none"> ● Puede vincular una EIP a una dirección IP virtual para permitir que los ECS con la dirección IP virtual enlazada accedan a Internet. ● Puede vincular una EIP a un ECS para permitir que el ECS acceda a Internet. Cada EIP puede estar vinculada a un solo ECS a la vez. <p>Para obtener más información, consulte la Descripción de EIP.</p>	<ul style="list-style-type: none"> ● Bind EIP (122.9.9.85) to virtual IP address (172.16.0.2) to enable ECS-A-01 and ECS-A-02 to access the Internet. ● Bind EIP (122.9.9.87) to ECS-B-01 to enable ECS-B-01 to access the Internet.

4.3 ¿Cómo accedo a Internet mediante un enlace de EIP a una NIC de extensión?

1. Una vez que una EIP está vinculada a una NIC de extensión, inicie sesión en el ECS y utilice el comando **route** para consultar la ruta.

Puede ejecutar **route --help** para obtener más información sobre el comando **route**.

Figura 4-2 Consulta de la información de la ruta

```
[root@ecs-b926 ~]# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          192.168.11.1   0.0.0.0        UG    0      0      0 eth0
169.254.0.0      0.0.0.0        255.255.0.0    U     1002   0      0 eth0
169.254.0.0      0.0.0.0        255.255.0.0    U     1003   0      0 eth1
169.254.169.254 192.168.11.1   255.255.255.255 UGH   0      0      0 eth0
192.168.11.0     0.0.0.0        255.255.255.0  U     0      0      0 eth0
192.168.17.0     0.0.0.0        255.255.255.0  U     0      0      0 eth1
[root@ecs-b926 ~]#
```

2. Ejecute el comando **ifconfig** para ver la información de la NIC.

Figura 4-3 Consulta de información de NIC

```
[root@ecs-b926 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.42 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::f816:3eff:fe7:1c44 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:f7:1c:44 txqueuelen 1000 (Ethernet)
    RX packets 127 bytes 21633 (21.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 258 bytes 22412 (21.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.191 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::f816:3eff:felc:b57f prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:1c:b5:7f txqueuelen 1000 (Ethernet)
    RX packets 11 bytes 1283 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1388 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 51 bytes 12018 (11.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 51 bytes 12018 (11.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. Habilite el acceso a Internet a través de la NIC de extensión de forma predeterminada.

- a. Ejecute el siguiente comando para eliminar la ruta predeterminada de la NIC principal:

```
route del -net 0.0.0.0 gw 192.168.11.1 dev eth0
```

NOTA

Esta operación interrumpirá la comunicación de ECS. Se recomienda que realice la configuración siguiendo el paso 4.

- b. Ejecute el siguiente comando para configurar la ruta predeterminada para la NIC de la extensión:

```
route add default gw 192.168.17.1
```

4. Configure el acceso a Internet desde la NIC de la extensión en función de su dirección de destino.

Ejecute el siguiente comando para configurar el acceso a un bloque CIDR especificado (por ejemplo, xx.xx.0.0/16) a través de la extensión NIC:

Puede configurar el bloque CIDR según sea necesario.

```
route add -net xx.xx.0.0 netmask 255.255.0.0 gw 192.168.17.1
```

4.4 ¿Cuáles son las diferencias entre las NIC primarias y de extensión de los ECS?

A continuación, se detallan las diferencias:

- Generalmente, las rutas predeterminadas de SO utilizan preferentemente las NIC primarias. Si las rutas predeterminadas de SO utilizan las NIC de extensión, la comunicación de red se interrumpirá. A continuación, puede comprobar la configuración de la ruta para rectificar el error de comunicación de red.

- Las NIC primarias pueden comunicarse con la zona de servicio público (zona donde se implementan los servicios PaaS y DNS). Las NIC de extensión no pueden comunicar esta zona.

4.5 ¿Se puede cambiar una EIP que usa ancho de banda dedicado para usar ancho de banda compartido?

Sí. Una EIP de pago por uso que utiliza el ancho de banda dedicado se puede cambiar para utilizar el ancho de banda compartido. Sin embargo, una EIP anual/mensual que utiliza el ancho de banda dedicado no se puede cambiar para utilizar el ancho de banda compartido.

4.6 ¿Puedo vincular una EIP a varios ECS?

Cada EIP puede estar vinculada a un solo ECS a la vez.

Varios ECS no pueden compartir una misma EIP. Un ECS y su EIP enlazada deben estar en la misma región. Si desea que varios ECS en la misma VPC compartan una EIP, debe usar un gateway de NAT. Para obtener más información, consulte la [Guía del usuario de NAT Gateway](#).

4.7 How Do I Access an ECS with an EIP Bound from the Internet?

Each ECS is automatically added to a security group after being created to ensure its security. The security group denies access traffic from the Internet by default (except TCP traffic from port 22 through SSH to a Linux ECS and TCP traffic from port 3389 through RDP to a Windows ECS). To allow external access to ECSs in the security group, add an inbound rule to the security group.

You can set **Protocol** to **TCP**, **UDP**, **ICMP**, or **All** as required on the page for creating a security group rule.

- If your ECS needs to be accessible over the Internet and you know the IP address used to access the ECS, set **Source** to the IP address range containing the IP address.
- If your ECS needs to be accessible over the Internet but you do not know the IP address used to access the ECS, retain the default setting 0.0.0.0/0 for **Source**, and then set allowed ports to improve network security.

The default source **0.0.0.0/0** indicates that all IP addresses can access ECSs in the security group.

- Allocate ECSs that have different Internet access requirements to different security groups.

4.8 ¿Qué es la política de asignación de EIP?

De forma predeterminada, las EIP se asignan aleatoriamente.

Si se libera una EIP por error, el sistema le asignará preferentemente una EIP que haya liberado en las últimas 24 horas.

Si no quieres una EIP que haya liberado, se recomienda que primero compre otra EIP y luego libere la que no necesite.

4.9 ¿Puedo vincular una EIP de un ECS a otro ECS?

Sí.

Puede desvincular la EIP del ECS original. Para obtener más información, consulte la sección [Desvinculación de una EIP de una instancia](#).

A continuación, une la EIP al ECS objetivo. Para obtener más información, consulte la sección [Vinculación de una EIP a una instancia](#).

Si desea cambiar un EIP para su ECS, consulte [Cambio de una EIP](#).

4.10 ¿Una EIP cambia con el tiempo?

Las EIP no se modificarán después de haber sido asignadas.

- Detener e iniciar un ECS no cambia su EIP.
- El cambio en el modo de facturación no cambia las EIP.

Una EIP se liberará si expira o si la cuenta del propietario de la EIP está en mora.

4.11 ¿Puedo comprar una específica?

De forma predeterminada, las EIP se asignan aleatoriamente. Si ha liberado las EIP, el sistema asigna preferentemente las EIP de las que ha liberado.

Puede asignar una EIP específica solo invocando a una API. Para obtener más información, consulte la sección [Asignar una EIP](#).

4.12 ¿Cómo puedo consultar la región de mis EIP?

Puede visitar <https://en.ipip.net/?origin=CN> para consultar la región de sus EIP.

- La región de una EIP identificada mediante un sitio web de terceros puede ser diferente de la región a la que pertenece la EIP.
- Si la región identificada mediante otro sitio web de terceros es diferente de la identificada mediante <https://en.ipip.net/?origin=CN>, utilice la región identificada por <https://en.ipip.net/?origin=CN>.
- Si la región identificada con <https://en.ipip.net/?origin=CN> es diferente de la que seleccionó al comprar la EIP, utilice la región que seleccionó durante la compra de la EIP.

NOTA

La ubicación geográfica de una EIP comprada en CN North-Ulanqab1 es Pekín.

- Si su servicio se ve afectado negativamente porque no se puede determinar la región de su EIP, [envíe un ticket de servicio](#).

Para saber más sobre la región de las EIP, [envíe un ticket de servicio](#).

4.13 ¿Puede un ancho de banda ser utilizado por varias cuentas?

Un ancho de banda no se puede compartir entre diferentes cuentas. Cada cuenta puede usar y gestionar solo sus propios anchos de banda de EIP.

4.14 ¿Cómo cambio una EIP para una instancia?

Escenario 1: Cambio de una EIP para un ECS

1. Desvincular una EIP.
 - a. Inicie sesión en la consola de gestión.
 - b. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
 - c. En la página mostrada, busque la fila que contiene la EIP de destino y haga clic en **Unbind**.
 - d. Haga clic en **Yes**.
2. Asignar una EIP.
 - a. Log in to the management console.
 - b. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
 - c. En la página mostrada, haga clic en **Buy EIP**.
 - d. Establezca los parámetros como se le solicite.
 - e. Haga clic en **Next**.
3. Vincular la nueva EIP al ECS.
 - a. Inicie sesión en la consola de gestión.
 - b. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
 - c. En la página **EIPs**, busque la fila que contiene el EIP de destino y haga clic en **Bind**.
 - d. Seleccione el ECS deseado.
 - e. Haga clic en **OK**.
4. Liberar la EIP que se ha reemplazado.
 - a. Inicie sesión en la consola de gestión.
 - b. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
 - c. En la lista de EIP, busque la fila que contiene la EIP de destino y haga clic en **Release**.
 - d. Haga clic en **Yes**.

Escenario 2: Cambio de una EIP para un balanceador de carga

1. Desvincular una EIP.
 - a. Inicie sesión en la consola de gestión.
 - b. Haga clic en **Service List**. En **Networking**, haga clic en **Elastic Load Balance**.

- c. En la lista de balanceadores de carga, localice el balanceador de carga de destino y elija **More > Unbind EIP** en la columna **Operation**.
 - d. Haga clic en **Yes**.
 2. Asignar una EIP haciendo referencia a [2](#).
 3. Vincular la nueva EIP al balanceador de carga.
 - a. Inicie sesión en la consola de gestión.
 - b. Haga clic en **Service List**. En **Networking**, haga clic en **Elastic Load Balance**.
 - c. En la lista de balanceadores de carga, localice el balanceador de carga de destino y elija **More > Bind EIP** en la columna **Operation**.
 - d. En el cuadro de diálogo **Bind EIP**, seleccione la EIP que desea vincular y haga clic en **OK**.
 4. Liberar la EIP que fue reemplazada. Para obtener más información, véase [4](#).

Escenario 3: Cambio de una EIP para un NAT Gateway

1. Asignar una EIP haciendo referencia a [2](#).
2. Modificar una regla de SNAT.

Para obtener más información, consulte la sección [Modificación de una regla de SNAT](#). En la lista de EIP, seleccione la nueva EIP y anule la selección de la EIP existente.
3. Modificar una regla de DNAT.

Para obtener más información, consulte la sección [Modificación de una regla de DNAT](#).
4. Liberar la EIP que fue reemplazada. Para obtener más información, véase [4](#).

4.15 ¿Puedo vincular una EIP a un recurso en la nube en otra región?

No. Las EIP y sus recursos asociados en la nube deben estar en la misma región.

4.16 ¿Puedo cambiar la región de mi EIP?

La región de una EIP no se puede cambiar.

Si ha asignado una EIP en la región A pero necesita una EIP en la región B, no puede cambiar directamente la región del EIP asignado de A a B. En su lugar, debe asignar una EIP en la región B.

5 Interconexiones de VPC

5.1 ¿Cuántas interconexiones de VPC puedo crear en una cuenta?

Si utiliza una interconexión de VPC para conectar VPC en la misma región, puede iniciar sesión en la consola de gestión para ver la cuota de la interconexión de VPC. Para más detalles, véase [¿Qué es una cuota?](#)

- Número de interconexiones de VPC que puede crear en cada región entre VPC en la misma cuenta: sujeto a la cuota real
- Número de interconexiones de VPC que puede crear en cada región entre VPC en diferentes cuentas: Las interconexiones de VPC aceptadas usan las cuotas de ambas cuentas. Las interconexiones de VPC que deben aceptarse solo usan las cuotas de cuentas que solicitan las conexiones.

Una cuenta puede crear interconexiones de VPC con diferentes cuentas si la cuenta tiene suficiente cuota.

5.2 ¿Una interconexión de VPC puede conectar las VPC en diferentes regiones?

Una interconexión de VPC solo puede conectar las VPC en la misma región.

5.3 ¿Por qué falló la comunicación entre las VPC que estaban conectadas por una interconexión de VPC?

Síntomas

Después de crear una interconexión de VPC, la VPC local y la emparejada no pueden comunicarse entre sí.

Resolución de problemas

Los problemas aquí se describen en orden de la probabilidad de que ocurran.

Tabla 5-1 Posibles causas y soluciones

N.º	Causa posible	Solución
1	<p>Bloques CIDR superpuestos de la VPC local y la emparejada</p> <ul style="list-style-type: none"> ● Todos sus bloques CIDR de subred se superponen. ● Algunos de sus bloques CIDR de subred se superponen. 	<p>Refiérase a Bloques CIDR superpuestos de la VPC local y la emparejada.</p>
2	<p>Configuración incorrecta de la ruta para la VPC local y la emparejada</p> <ul style="list-style-type: none"> ● No se agrega ninguna ruta. ● Se agregan rutas incorrectas. ● Los destinos de las rutas se superponen con los configurados para Direct Connect o conexiones de VPN. 	<p>Refiérase a Configuración de ruta incorrecta para la VPC local y la emparejada.</p>
3	<p>Configuración incorrecta de red</p> <ul style="list-style-type: none"> ● Las reglas de grupo de seguridad de los ECS que necesitan comunicarse niegan el tráfico entrante entre sí. ● El firewall de la NIC de ECS bloquea el tráfico. ● Las reglas de ACL de red de las subredes conectadas por la interconexión de VPC niegan el tráfico entrante. ● Compruebe la configuración del enrutamiento basado en políticas de un ECS con varias NIC. 	<p>Refiérase a Configuración de red incorrecta.</p>
4	<p>Error de red de ECS</p>	<p>Refiérase a Error de red de ECS.</p>

AVISO

Si el problema persiste, [envíe un ticket de servicio](#).

Bloques CIDR superpuestos de la VPC local y la emparejada

Si los bloques CIDR de VPC conectados por una interconexión de VPC se superponen, la conexión no tiene efecto debido a los conflictos de ruta.

Tabla 5-2 Bloques CIDR superpuestos de la VPC local y la emparejada

Escenario	Descripción	Solución
Las VPC con los bloques CIDR superpuestos también incluyen subredes que se superponen.	los bloques CIDR de VPC-A y VPC-B se superponen, y todas sus subredes se superponen. <ul style="list-style-type: none"> ● Bloques CIDR superpuestos de VPC-A y VPC-B: 10.0.0.0/16 ● Bloques CIDR superpuestos de Subnet-A01 en VPC-A y Subnet-B01 en VPC-B: 10.0.0.0/24 ● Bloques CIDR superpuestos de Subnet-A02 en VPC-A y Subnet-B02 en VPC-B: 10.0.1.0/24 	VPC-A y VPC-B no se pueden conectar mediante una interconexión de VPC. Vuelva a planificar la red.
Dos VPC tienen bloques CIDR superpuestos, pero algunas de sus subredes no se superponen.	los bloques CIDR de VPC-A y VPC-B se superponen, y algunas de sus subredes se superponen. <ul style="list-style-type: none"> ● Bloques CIDR superpuestos de VPC-A y VPC-B: 10.0.0.0/16 ● Bloques CIDR superpuestos de Subnet-A01 en VPC-A y Subnet-B01 en VPC-B: 10.0.0.0/24 ● Los bloques CIDR de la Subnet-A02 en VPC-A y la Subnet-B02 en VPC-B no se superponen. 	<ul style="list-style-type: none"> ● Una interconexión de VPC no puede conectar todas las VPC, VPC-A y VPC-B. ● Una conexión puede conectar sus subredes (Subnet-A02 y Subnet-B02) que no se superponen.

Si los bloques CIDR de las VPC se superponen y algunas de sus subredes se superponen, puede crear una interconexión de VPC entre sus subredes con bloques CIDR no superpuestos.

Tabla 5-3 Rutas requeridas para la interconexión de VPC entre la Subnet-A02 y la Subnet-B02

Tabla de rutas	Destino	Salto siguiente	Descripción
Tabla de ruta de VPC-A	10.0.2.0/24	Peering-AB	Agregue una ruta con el bloque CIDR de la Subnet-B02 como destino y Peering-AB como el salto siguiente.
Tabla de ruta de VPC-B	10.0.1.0/24	Peering-AB	Agregue una ruta con el bloque CIDR de la Subnet-A02 como destino y Peering-AB como el salto siguiente.

AVISO

- Si una interconexión de VPC entre las VPC con bloques CIDR superpuestos no tiene efecto, consulte [Configuraciones no compatibles de la interconexión de VPC](#).
- Si dos VPC desean utilizar sus bloques CIDR IPv6 para la comunicación a través de una interconexión de VPC pero sus bloques CIDR IPv4 o subredes se superponen, la conexión no es utilizable.

Configuración de ruta incorrecta para la VPC local y la emparejada

Consulta las rutas en la tabla de rutas de la VPC local y la emparejada. [Tabla 5-4](#) lista los elementos que necesita comprobar.

Tabla 5-4 Elementos de comprobación de ruta

Concepto	Solución
Compruebe si las rutas se agregan a la tabla de rutas de la VPC locales y la emparejada.	Si no se agregan rutas, agregue rutas haciendo referencia a: <ul style="list-style-type: none"> ● Creating a VPC Peering Connection with Another VPC in Your Account ● Creación de una interconexión de VPC con una VPC en otra cuenta
Compruebe los destinos de las rutas agregadas a la tabla de rutas de la VPC local y la emparejada. <ul style="list-style-type: none"> ● In the route table of the local VPC, check whether the route destination is the CIDR block, subnet CIDR block, or related private IP address of the peer VPC. ● En la tabla de ruta de la VPC emparejada, compruebe si el destino de la ruta es el bloque CIDR, el bloque CIDR de la subred o la dirección IP privada relacionada de la VPC local. 	Si el destino de la ruta es incorrecto, cámbielo .
Los destinos de las rutas se superponen con los configurados para Direct Connect o conexiones de VPN.	Compruebe si alguna de las VPC conectadas por la interconexión de VPC también tiene una conexión de VPN o de Direct Connect conectada. Si lo hacen, compruebe los destinos de sus rutas. Si los destinos de las rutas se superponen, la interconexión de VPC no tiene efecto. En este caso, vuelva a planificar la conexión de red.

Configuración de red incorrecta

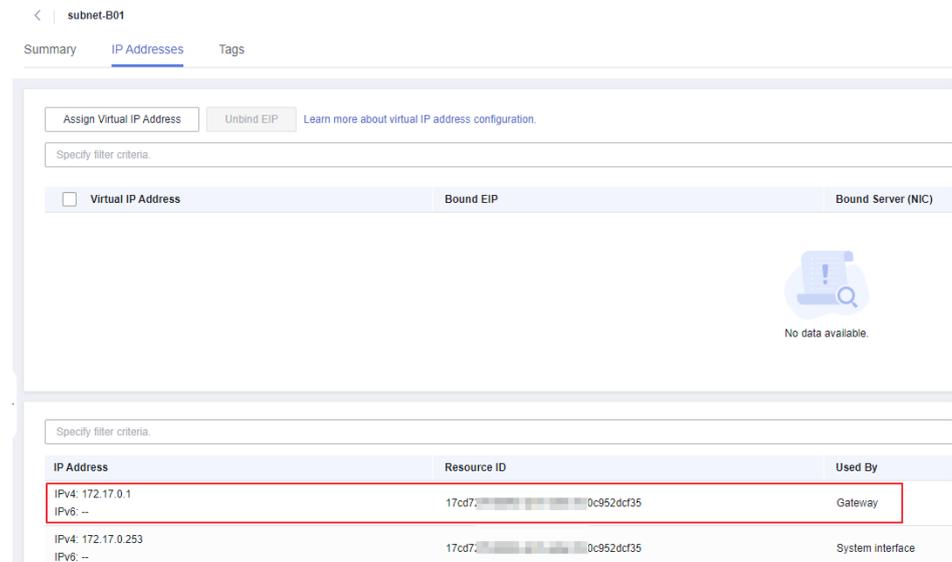
1. **Compruebe si las reglas de grupo de seguridad de los ECS que necesitan comunicarse permiten el tráfico entrante entre sí.**
 - Si los ECS están asociados con el mismo grupo de seguridad, no es necesario comprobar sus reglas.
 - Si los ECS están asociados con diferentes grupos de seguridad, **agregue una regla de entrada para permitir el acceso entre sí.**
2. Compruebe si el firewall de la NIC de ECS bloquea el tráfico.
Si el firewall bloquea el tráfico, configure el firewall para permitir el tráfico entrante.
3. Compruebe si las reglas de ACL de red de las subredes conectadas por la interconexión de VPC niegan el tráfico entrante.
Si las reglas de ACL de red niegan el tráfico entrante, configure las reglas para permitir el tráfico.
4. Si un ECS tiene más de una NIC, compruebe si el enrutamiento basado en políticas correcto se ha configurado para el ECS y los paquetes con diferentes direcciones IP de origen coinciden con sus propias rutas de cada NIC.
Si un ECS tiene dos NIC (eth0 y eth1):
 - Dirección IP de eth0: 192.168.1.10; Gateway de subred: 192.168.1.1
 - Dirección IP de eth1: 192.168.2.10; Gateway de subred: 192.168.2.1Formatos de los comandos:
 - **ping -I IP address of eth0 Subnet gateway address of eth0**
 - **ping -I IP address of eth1 Subnet gateway address of eth1**Ejecute los siguientes comandos:
 - **ping -I 192.168.1.10 192.168.1.1**
 - **ping -I 192.168.2.10 192.168.2.1**Si la comunicación de red es normal, las rutas de las NIC se configuran correctamente.
De lo contrario, **debe configurar el enrutamiento basado en políticas para el ECS con varias NIC**.

Error de red de ECS

1. Inicie sesión en el ECS.
2. Compruebe si la NIC de ECS tiene una dirección IP asignada.
 - ECS de Linux: Utilice el comando **ifconfig** o **ip address** para ver la dirección IP de la NIC.
 - ECS de Windows: En el cuadro de búsqueda, escriba **cmd** y pulse **Enter**. En el símbolo del sistema que se muestra, ejecute el comando **ipconfig**.Si la NIC de ECS no tiene una dirección IP asignada, consulte [¿Por qué mi ECS no puede obtener una dirección IP?](#)
3. Compruebe si el gateway de la subred del ECS se puede hacer ping.
 - a. En la lista de ECS, haga clic en el nombre de ECS.
Se muestra la página de detalles de ECS.
 - b. En la página de detalles de ECS, haga clic en el hipervínculo de VPC.
Se muestra la página **Virtual Private Cloud**.

- c. En la lista de VPC, busque la VPC de destino y haga clic en el número en la columna **Subnets**.
Se muestra la página **Subnets**.
- d. En la lista de subred, haga clic en el nombre de la subred.
Se muestra la página de detalles de subred.
- e. Haga clic en la ficha **IP Addresses** y vea la dirección de gateway de la subred.

Figura 5-1 Dirección del gateway



- f. Compruebe si la comunicación del gateway es normal:

ping *Subnet gateway address*

Comando de ejemplo: **ping 172.17.0.1**

Si la dirección del gateway no se puede hacer ping, consulte [¿Por qué mi ECS no se comunica en una red de nivel 2 o 3?](#)

6 Direcciones IP virtuales

6.1 ¿Por qué no se puede hacer ping a la dirección IP virtual después de vincularla a una NIC de ECS?

Síntomas

Después de vincular una dirección IP virtual a una NIC de ECS, no puede hacer ping a la dirección IP virtual.

Resolución de problemas

Los problemas aquí se describen en orden de la probabilidad de que ocurran.

Solucione el problema descartando las causas descritas aquí, una por una.

Figura 6-1 Resolución de problemas

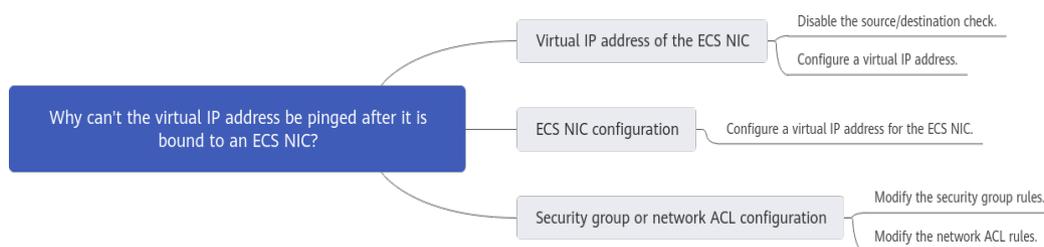


Tabla 6-1 Resolución de problemas

Causa posible	Solución
Dirección IP virtual de la NIC de ECS	Consulte Dirección IP virtual de la NIC de ECS
Dirección IP virtual de la NIC interna del ECS	Consulte Dirección IP virtual de la NIC interna del ECS

Causa posible	Solución
Configuración de ACL de grupo de seguridad o red	Consulte Configuración de ACL de grupo de seguridad o red

Dirección IP virtual de la NIC de ECS

Compruebe si la comprobación de origen/destino de la NIC está deshabilitada y si una dirección IP virtual está vinculada a la NIC.

1. Inicie sesión en la consola de gestión.
2. Haga clic en **Service List** y haga clic en **Elastic Cloud Server** en **Computing**.
3. En la lista de ECS, haga clic en el nombre del ECS.
4. En la página de detalles de ECS que se muestra, haga clic en la ficha **Network Interfaces**.
5. Asegúrese de que **Source/Destination Check** esté deshabilitada.
6. Asegúrese de que se muestra una dirección IP para **Virtual IP Address** en la página de detalles de la NIC.

Si no hay una dirección IP virtual, haga clic en **Manage Virtual IP Address**. En la ficha **IP Addresses** mostrada, haga clic en **Assign Virtual IP Address**.

📖 NOTA

Para comprobar si se ha configurado una dirección IP virtual, **ifconfig** no funcionará. Utilice **ip address** en su lugar. Para obtener más información, consulte [Vinculación de una dirección IP virtual a una EIP o a un ECS](#).

Dirección IP virtual de la NIC interna del ECS

A continuación se utilizan los ECS de Linux y de Windows como ejemplos para describir cómo comprobar si una NIC de ECS tiene una dirección IP virtual.

Para un ECS de Linux:

1. Compruebe si hay una NIC **ethX:X**:

ifconfig

Figura 6-2 Comprobación de NIC **ethX:X**

```
[root@scy ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::f816:3eff:fe4d:5b98 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:4d:5b:98 txqueuelen 1000 (Ethernet)
    RX packets 77399 bytes 5101164 (4.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68798 bytes 8090922 (7.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.137 netmask 255.255.255.0 broadcast 192.168.1.255
    ether fa:16:3e:4d:5b:98 txqueuelen 1000 (Ethernet)
```

El resultado del comando en la figura anterior contiene un NIC **ethX:X. 192.168.1.137** es su dirección IP virtual.

- Si la NIC **ethX:X** está allí, la NIC de ECS está correctamente configurada.
 - Si no se encuentra el NIC **ethX:X**, realice las siguientes operaciones:
2. Si la salida del comando no contiene una NIC **ethX:X**, cambie al directorio **/etc/sysconfig/network-scripts**:
cd /etc/sysconfig/network-scripts
 3. Ejecute el siguiente comando para crear y luego modificar el archivo **ifcfg-eth0:1**:
vi ifcfg-eth0:1

Agregue la siguiente información de NIC al archivo:

```
BOOTPROTO=static
DEVICE=eth0:1
HWADDR=fa:16:3e:4d:5b:98
IPADDR=192.168.1.137
GATEWAY=192.168.1.1
NETMASK=255.255.255.0
ONBOOT=yes
ONPARENT=yes
```

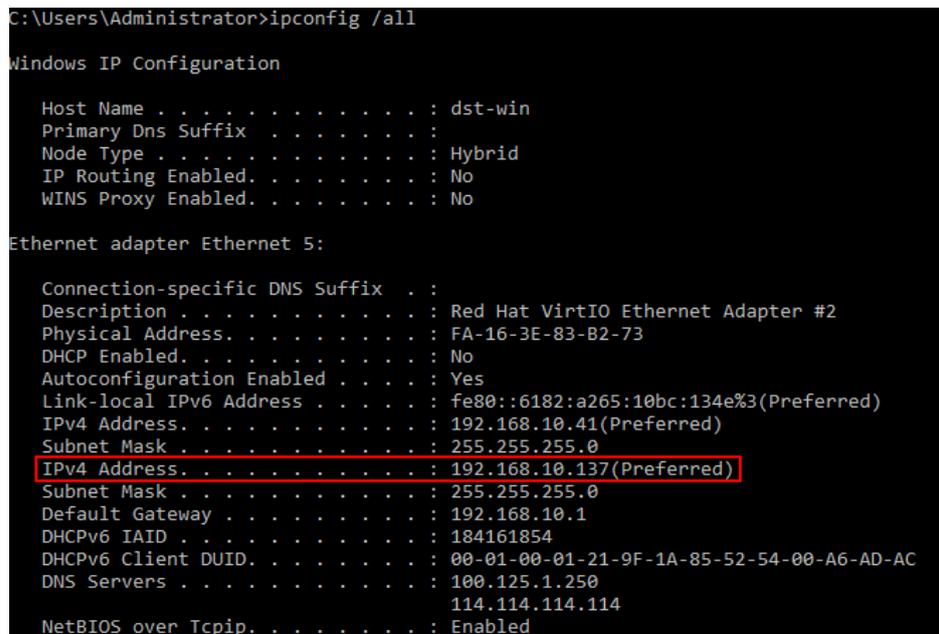
4. Presione **Esc**, escriba **:wq!**, guarde el archivo y salga.
5. Reinicie el ECS y ejecute el comando **ifconfig** para comprobar si la dirección IP virtual se ha configurado para el ECS.

Para un ECS de Windows:

1. En el menú **Start**, abra la ventana de línea de comandos de Windows y ejecute el siguiente comando para comprobar si se ha configurado la dirección IP virtual:

ipconfig /all

Figura 6-3 Comprobación de si se ha configurado la dirección IP virtual



```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : dst-win
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

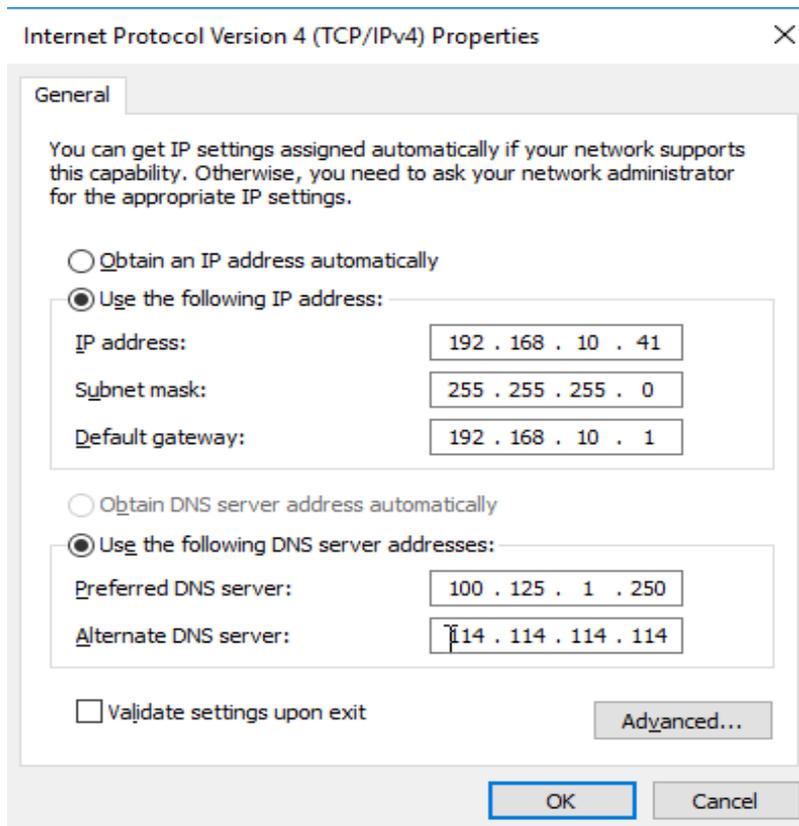
Ethernet adapter Ethernet 5:

Connection-specific DNS Suffix . :
Description . . . . . : Red Hat VirtIO Ethernet Adapter #2
Physical Address. . . . . : FA-16-3E-83-B2-73
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6182:a265:10bc:134e%3(Preferred)
IPv4 Address. . . . . : 192.168.10.41(Preferred)
Subnet Mask . . . . . : 255.255.255.0
IPv4 Address. . . . . : 192.168.10.137(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
DHCPv6 IAID . . . . . : 184161854
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-9F-1A-85-52-54-00-A6-AD-AC
DNS Servers . . . . . : 100.125.1.250
                          114.114.114.114
NetBIOS over Tcpip. . . . . : Enabled
```

En la salida del comando anterior, compruebe si el valor de la **IPv4 Address** (192.168.10.137) es la dirección IP de la NIC de ECS.

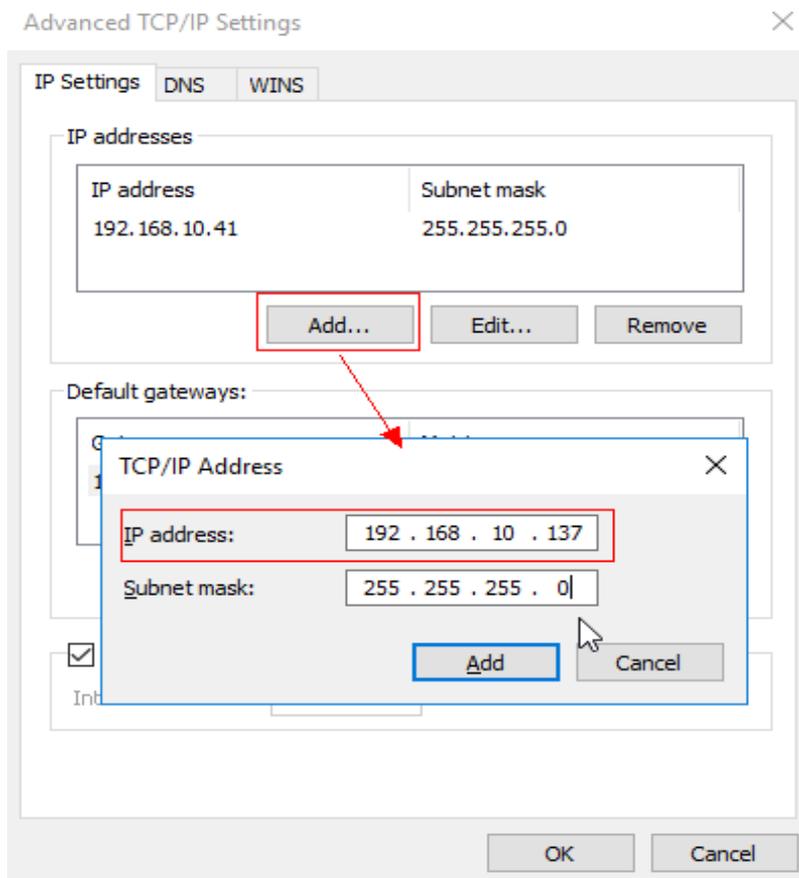
- En caso afirmativo, se ha configurado la dirección IP virtual para la NIC de ECS.
 - En caso negativo, realice las siguientes operaciones:
2. Seleccione **Control Panel > Network and Internet > Network Connections**. Haga clic con el botón secundario en la conexión local correspondiente y, a continuación, haga clic en **Properties**.
 3. En la página **Network**, seleccione **Internet Protocol Version 4 (TCP/IPv4)**.
 4. Haga clic en **Properties**.
 5. Seleccione **Use the following IP address** y establezca **IP address** en la dirección IP privada que se muestra en **Figura 6-3**. Por ejemplo, 192.168.10.41.

Figura 6-4 Configuración de una dirección IP privada



6. Haga clic en **Advanced**.
7. En la pestaña **IP Settings**, haga clic en **Add** en el área **IP addresses**. Agregue la dirección IP virtual configurada en el **Figura 6-3**. Por ejemplo, 192.168.10.137.

Figura 6-5 Configuración de la dirección IP virtual



Configuración de ACL de grupo de seguridad o red

Compruebe si los grupos de seguridad de ECS y las ACL de red asociadas a la subred utilizada por la NIC de ECS están bloqueando el tráfico.

1. En la página de detalles de ECS, haga clic en la ficha **Security Groups** y confirme que se han configurado las reglas de grupo de seguridad necesarias para la dirección IP virtual. Si no se han configurado las reglas de grupo de seguridad necesarias, haga clic en **Change Security Group** o **Modify Security Group Rule** para cambiar el grupo de seguridad o modificar las reglas de grupo de seguridad.
2. Haga clic en **Service List**. En **Networking**, haga clic en **Virtual Private Cloud**. En el panel de navegación a la izquierda de la consola de red, haga clic en **Network ACLs** y compruebe si las reglas de ACL de red asociadas a la subred utilizada por la NIC de ECS están bloqueando el acceso a la dirección IP virtual.

Envío de un ticket de servicio

Si el problema persiste, [envíe un ticket de servicio](#).

6.2 ¿Cómo puedo vincular una dirección IP virtual en Huawei Cloud a un servidor en un centro de datos local?

Prerrequisitos

- Ha asignado las direcciones IP virtuales. Para obtener más información, consulte [Asignación de una dirección IP virtual](#).
- Ha creado una conexión de capa 2 para la subred donde reside la dirección IP virtual. Para obtener más información, consulte [Compra de un conmutador empresarial](#).

Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
3. En el árbol de navegación de la izquierda, seleccione **Conmutador de empresa**.
4. Haga clic en **Manage Virtual IP Address** a la derecha de **Layer 2 Connection Topology**.
5. En la lista Dirección IP, busque la fila que contiene la dirección IP virtual de destino y haga clic en **Bind to Instance** en la columna **Operation**.
6. En la página **Bind to Instance**, establezca **Instance Type** en **Layer 2 Connection**, seleccione la conexión de Capa 2 de destino y haga clic en **OK**.

6.3 ¿Por qué la red está desconectada entre los servidores usando una dirección IP virtual después de una conmutación activa/en espera?

Para un clúster de HA configurado con direcciones IP virtuales y Keepalived, si encuentra que la red entre el cliente y el servidor está desconectada después de una conmutación activa/en espera, la causa posible es que la conmutación se realiza manualmente. Como resultado, la tabla ARP del cliente no se actualiza, puede realizar las siguientes operaciones para actualizar la tabla de ARP:

1. Inicie sesión en el cliente.
2. Actualice la tabla de ARP en el cliente.
 - Método 1: Activar el cliente para que aprenda la nueva dirección de MAC correspondiente a la dirección IP virtual:
ping *Virtual IP address*
Comando de ejemplo: **ping 192.168.3.22**
 - Método 2: Borrar las entradas residuales en la tabla de ARP de la dirección IP virtual para activar el cliente para aprender la nueva tabla ARP:
arp -d *Virtual IP address*
Ejemplo de comando: **arp -d 192.168.3.22**

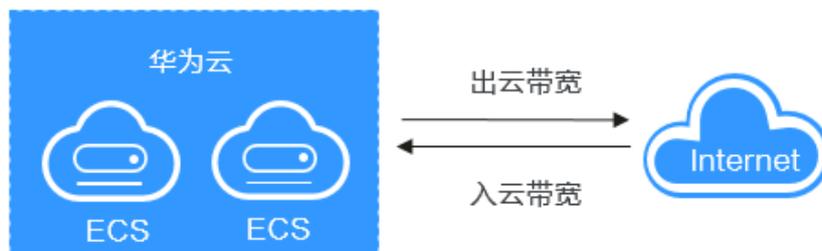
7 Ancho de banda

7.1 ¿Qué son el ancho de banda entrante y el ancho de banda saliente?

El ancho de banda entrante es el ancho de banda consumido cuando los datos se transfieren desde Internet a Huawei Cloud. Por ejemplo, cuando se descargan recursos de Internet a los ECS, eso consume ancho de banda entrante.

El ancho de banda saliente es el ancho de banda consumido cuando los datos se transfieren desde Huawei Cloud a Internet. Por ejemplo, cuando los ECS proporcionan los servicios accesibles desde Internet y los usuarios externos descargan recursos de los ECS, eso consume el ancho de banda saliente.

Figura 7-1 Ancho de banda entrante y ancho de banda saliente



Huawei Cloud solo factura el ancho de banda saliente.

NOTA

- Las reglas de límite para los anchos de banda públicos se cambiaron el 31 de julio de 2020, 00:00:00 GMT+08:00 en las regiones continentales de China, incluyendo CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, y CN North-Ulanqab1.

Las reglas de límite para anchos de banda públicos se cambiaron el 10 de diciembre de 2021, 00:00:00 GMT+08:00 en la región CN-Hong Kong.

Después del cambio:

- Si el ancho de banda adquirido o modificado es de hasta 10 Mbit/s, el ancho de banda entrante será de 10 Mbit/s, y el ancho de banda saliente será el mismo que el ancho de banda adquirido o modificado.
- Si el ancho de banda adquirido o modificado es más de 10 Mbit/s, ambos anchos de banda en las direcciones entrantes y salientes serán los mismos que el ancho de banda comprado o modificado.

7.2 ¿Cómo sé si se ha superado el límite de ancho de banda de mi EIP?

Síntomas

El tamaño de ancho de banda configurado al comprar un ancho de banda dedicado o compartido es el límite superior del ancho de banda saliente. Si no se puede acceder sin problemas a un ECS que ejecuta sus aplicaciones web desde Internet, compruebe si el ancho de banda saliente de la EIP vinculada al ECS es mayor que el tamaño de ancho de banda configurado.

NOTA

Si el ancho de banda saliente excede el tamaño de ancho de banda configurado, puede haber pérdida de paquetes. Para evitar la pérdida de datos, se recomienda supervisar el ancho de banda.

Resolución de problemas

Los problemas aquí se describen en orden de la probabilidad de que ocurran.

Solucione el problema descartando las causas descritas aquí, una por una.

Figura 7-2 Resolución de problemas

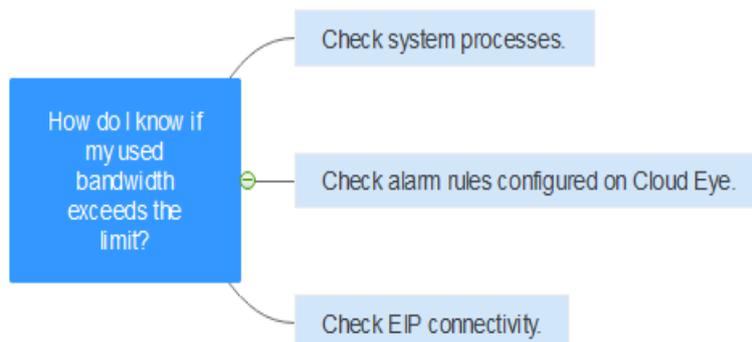


Tabla 7-1 Resolución de problemas

Causa posible	Descripción	Solución
Procesos del sistema que conducen a un alto ancho de banda	Si algunos procesos o aplicaciones del sistema de servicio pesado que se ejecutan en su ECS están causando el alto ancho de banda o uso de CPU, su ECS se ejecutará lentamente o puede ser inesperadamente inaccesible.	Consulte Procesos del sistema que conducen al uso de alto ancho de banda
Reglas inadecuadas de la alarma de Cloud Eye	Si ha creado reglas de alarma para el uso del ancho de banda en la consola de Cloud Eye, donde el límite de ancho de banda de salida o el período de alarma es demasiado pequeño, el sistema puede generar alarmas excesivas.	Consulte Reglas inadecuadas de la alarma de Cloud Eye
Error de conexión de EIP	Un ECS con una EIP enlazada no puede acceder a Internet.	Vea ¿Por qué mi ECS no puede acceder a Internet incluso después de que una EIP está vinculada?

Procesos del sistema que conducen al uso de alto ancho de banda

Si algunos procesos o aplicaciones del sistema de servicio pesado que se ejecutan en su ECS están causando el alto ancho de banda o uso de CPU, su ECS se ejecutará lentamente o puede ser inesperadamente inaccesible.

Puede consultar lo siguiente para localizar los procesos que han llevado a un uso excesivo de ancho de banda o CPU, y optimizar o detener los procesos.

- [¿Por qué mi ECS de Windows se ejecuta lentamente?](#)
- [¿Por qué mi ECS de Linux se ejecuta lentamente?](#)

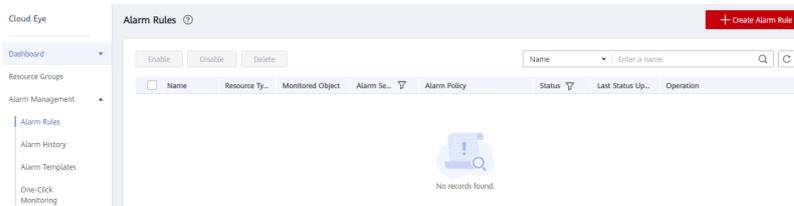
Reglas inadecuadas de la alarma de Cloud Eye

Si ha creado reglas de alarma para el uso del ancho de banda en la consola de Cloud Eye, donde el límite de ancho de banda de salida o el período de alarma es demasiado pequeño, el sistema puede generar alarmas excesivas.

Es necesario establecer una regla de alarma adecuada basada en el ancho de banda de compra. Por ejemplo, si el ancho de banda adquirido es de 5 Mbit/s, puede crear una regla de alarma para informar de una alarma cuando el ancho de banda de salida máximo alcance 4.8 Mbit/s tres períodos seguidos. También puede [aumentar su ancho de banda](#).

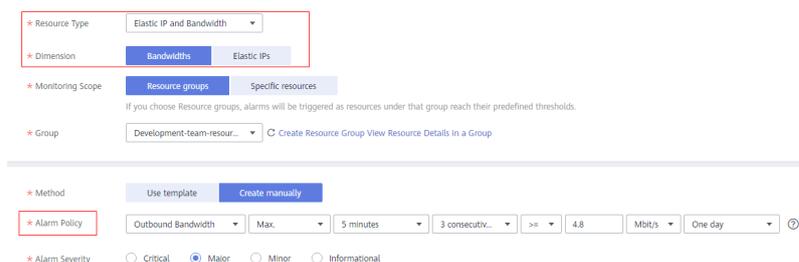
1. Inicie sesión en la consola de gestión, en **Management & Deployment**, haga clic en **Cloud Eye**. En la consola de **Cloud Eye**, elija **Alarm Management > Alarm Rules**.

Figura 7-3 Reglas de alarmas



2. Haga clic en **Create Alarm Rule** y configure una regla de alarma para generar alarmas cuando el ancho de banda exceda el límite configurado.

Figura 7-4 Creación de una regla de alarma



7.3 ¿Cuáles son las diferencias entre el ancho de banda de EIP y el ancho de banda de la red privada?

Los ECS utilizan los anchos de banda de EIP para acceder a Internet a través de EIP. Los anchos de banda de EIP utilizados serán facturados.

Los anchos de banda de la red privada se utilizan para la comunicación entre los ECS. El ancho de banda de red privada y la velocidad de transferencia de datos máxima (en PPS) permitida para un ECS se determinan basándose en las especificaciones de ECS.

Para obtener más información, consulte [Tipos de ECS](#).

7.4 ¿Cuál es el rango de tamaño del ancho de banda?

El rango de ancho de banda es de 1 Mbit/s a 2000 Mbit/s.

7.5 ¿Qué tipos de ancho de banda están disponibles?

Hay ancho de banda dedicado y ancho de banda compartido. Un ancho de banda dedicado solo puede ser utilizado por una EIP, pero un ancho de banda compartido puede ser utilizado por múltiples EIP.

7.6 ¿Cuáles son las diferencias entre un ancho de banda dedicado y un ancho de banda compartido?

Un ancho de banda dedicado solo puede ser utilizado por una EIP. Una EIP solo puede ser utilizada por un recurso en la nube, como un ECS, un gateway de NAT o un balanceador de carga.

Un ancho de banda compartido puede ser compartido por múltiples EIPs de pago por uso. Agregar una EIP a o quitar una EIP de un ancho de banda compartido no afecta a las cargas de trabajo.

Un ancho de banda dedicado no se puede cambiar a un ancho de banda compartido o al revés. Puede comprar un ancho de banda compartido para sus EIP de pago por uso.

- Después de agregar una EIP a un ancho de banda compartido, la EIP utilizará el ancho de banda compartido.
- Después de eliminar una EIP de un ancho de banda compartido, la EIP utilizará el ancho de banda dedicado.

7.7 ¿Cómo puedo comprar un ancho de banda compartido?

1. Inicie sesión en la consola de gestión.
2. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth > Shared Bandwidths**.
3. En la esquina superior derecha, haga clic en **Buy Shared Bandwidth**. En la página mostrada, configure los parámetros según se le solicite para comprar un ancho de banda compartido.

7.8 ¿Hay un límite en el número de las EIP que se pueden agregar a cada ancho de banda compartido?

Se puede agregar un máximo de 20 EIP a cada ancho de banda compartido. Si desea agregar más EIP a cada ancho de banda compartido, [envíe un ticket de servicio](#) a solicitar un aumento de cuota.

7.9 ¿Puedo aumentar mi ancho de banda facturado anualmente/mensualmente y luego disminuirlo?

Puede aumentar el ancho de banda para una EIP anual/mensual en cualquier momento que desee, y el cambio entra en vigor inmediatamente. Pero solo puede reducirlo cuando renueve la suscripción de EIP, y el ancho de banda reducido no tendrá efecto hasta el próximo ciclo de facturación. Para obtener más información, consulte [Modificación de un ancho de banda de EIP](#).

7.10 ¿Cuál es la relación entre el ancho de banda y la tasa de carga/descarga?

El ancho de banda se mide en bit/s, pero la velocidad de descarga se mide en byte/s.

1 byte = 8 bits, es decir, velocidad de descarga = ancho de banda/8

Debido a varios problemas como el rendimiento del equipo, la calidad del dispositivo de red, el uso de recursos y las horas pico de la red, si el ancho de banda es de 1 Mbit/s, la velocidad real de carga o descarga es generalmente inferior a 125 kByte/s (1 Mbit/s = 1,000 Kbit/s, velocidad de carga o descarga = 1,000/8 = 125 kByte/s).

7.11 ¿Cuáles son las diferencias entre BGP estático, BGP dinámico y BGP premium?

Las diferencias entre BGP estático, BGP dinámico y BGP premium son las siguientes:

Tabla 7-2 Diferencias entre BGP estático, BGP dinámico y BGP premium

Artículo	BGP estático	BGP dinámico	BGP Premium
Definición	Las rutas estáticas se configuran manualmente y deben reconfigurarse manualmente cada vez que cambie la topología de red o el estado del enlace.	El BGP dinámico proporciona conmutación por error automática y elige la ruta óptima según las condiciones de red en tiempo real, así como las políticas preestablecidas.	BGP premium elige la ruta óptima y garantiza redes de baja latencia y alta calidad. BGP se utiliza para interconectar con líneas de múltiples portadoras principales. Las conexiones de red pública que cuentan con baja latencia y alta calidad se establecen directamente entre China continental y Hong Kong (China). NOTA BGP premium ahora solo está disponible en la región CN-Hong Kong.

Artículo	BGP estático	BGP dinámico	BGP Premium
Garantía	<p>Cuando se producen cambios en una red que utiliza BGP estático, la configuración manual lleva algún tiempo y no se puede garantizar una alta disponibilidad.</p> <p>NOTA Si selecciona BGP estático, el sistema de aplicaciones debe tener configuraciones de recuperación ante desastres.</p>	<p>Cuando se produce un fallo en el enlace de un operador, el BGP dinámico seleccionará rápidamente otra ruta óptima para asumir los servicios, asegurando la disponibilidad del servicio.</p> <p>Actualmente, los operadores de China que soportan enrutamiento dinámico BGP incluyen China Telecom, China Mobile, China Unicom, China Education and Research Network (CERNET), National Radio and Television Administration, y Dr. Peng Group.</p>	<p>BGP premium tiene la misma capacidad de aseguramiento que el BGP dinámico.</p> <p>Además, BGP premium garantiza una mayor calidad de red y una menor latencia.</p> <p>Actualmente, los operadores principales en Hong Kong (China) son compatibles.</p>
Disponibilidad del servicio	99%	99.95%	99.95%
Facturación	Su precio de menos a más caro: BGP estático, BGP dinámico y BGP premium.		

8 Conectividad

8.1 ¿Permite una VPN la comunicación entre dos VPC?

If the two VPCs are in the same region, you can use a VPC peering connection to enable communication between them.

If the two VPCs are in different regions, you can use a VPN to enable communication between the VPCs. The CIDR blocks of the two VPCs are the local and remote subnets, respectively.

8.2 ¿Por qué Internet o los nombres de dominio internos en la nube son inaccesibles a través de nombres de dominio cuando mi ECS tiene varias NIC?

Cuando un ECS tiene más de una NIC, si se configuran diferentes direcciones de servidor de DNS para las subredes utilizadas por las NIC, el ECS no puede acceder a Internet ni a los nombres de dominio en la nube.

Puede resolver este problema configurando la misma dirección de servidor DNS para las subredes utilizadas por el mismo ECS. Puede realizar los siguientes pasos para modificar las direcciones del servidor de DNS de las subredes en una VPC:

1. Inicie sesión en la consola de gestión.
2. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
3. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
4. En la página **Virtual Private Cloud**, busque la VPC para la que se va a modificar una subred y haga clic en el nombre de la VPC.
5. En la lista de subred, busque la fila que contiene la subred que se va a modificar y haga clic en **Modify**. En la página mostrada, cambie la dirección del servidor DNS según se le solicite.
6. Haga clic en **OK**.

8.3 ¿Cuáles son las prioridades de la ruta personalizada y la EIP si ambas están configuradas para que un ECS permita que el ECS acceda a Internet?

La prioridad de una EIP es mayor que la de una ruta personalizada en una tabla de rutas de VPC. Por ejemplo:

La tabla de ruta de VPC de un ECS tiene una ruta personalizada con 0.0.0.0/0 como destino y el gateway de NAT como el salto siguiente.

Si un ECS en la VPC tiene una EIP vinculada, la tabla de ruta de VPC tendrá una ruta basada en políticas con 0.0.0.0/0 como destino, que tiene una prioridad más alta que su ruta personalizada. En este caso, el tráfico se reenvía a la EIP y no puede alcanzar el gateway de NAT.

8.4 ¿Por qué hay interrupciones intermitentes cuando un host local accede a un sitio web construido en un ECS?

Síntoma

Después de crear un sitio web en un ECS, algunos usuarios ocasionalmente no pueden acceder al sitio web a través de la red local.

Resolución de problemas

1. Compruebe la red local del usuario.
Si el host local se comunica con el ECS usando NAT, este problema puede ocurrir.
2. Ejecute el siguiente comando para comprobar si **tcp_tw_recycle** está habilitado en el ECS:
sysctl -a|grep tcp_tw_recycle
Si el valor de **tcp_tw_recycle** es **1**, la función está habilitada.
3. Ejecute el siguiente comando para comprobar el número de paquetes perdidos del ECS:
cat /proc/net/netstat | awk '/TcpExt/ { print \$21,\$22 }'
Si el valor de **ListenDrops** no es 0, hay pérdida de paquetes, es decir, la red está defectuosa.

Procedimiento

Este problema se puede resolver modificando los parámetros del núcleo del ECS.

- Ejecute el siguiente comando para modificar temporalmente los parámetros (los parámetros volverán a cambiar después de reiniciar):
sysctl -w net.ipv4.tcp_tw_recycle=0
- Realice las siguientes operaciones para modificar permanentemente los parámetros:
 - a. Ejecute el siguiente comando y modifique el archivo **/etc/sysctl.conf**:
vi /etc/sysctl.conf

Agregue el siguiente contenido al archivo:

```
net.ipv4.tcp_tw_recycle=0
```

- b. Presione **Esc**, escriba **:wq!**, guarde el archivo y salga.
- c. Ejecute el siguiente comando para hacer que la modificación surta efecto:
sysctl -p

8.5 ¿Por qué los ECS que utilizan las direcciones IP privadas en la misma subred solo admiten la comunicación unidireccional?

Síntoma

Dos ECS (**ecs01** y **ecs02**) están en la misma subred en una VPC. Sus direcciones IP son 192.168.1.141 y 192.168.1.40.

El **ecs01** puede hacer ping a **ecs02** a través de una dirección IP privada con éxito, pero **ecs02** no puede hacer ping a **ecs01** a través de una dirección IP privada.

Resolución de problemas

1. Ping **ecs01** desde **ecs02** hasta EIP. Si se puede hacer ping a **ecs01**, la NIC de **ecs01** funciona correctamente.
2. Ejecute el comando **arp -n** en **ecs02** para comprobar si la salida del comando contiene la dirección MAC de **ecs01**. Si la salida del comando no contiene la dirección MAC de **ecs01**, **ecs02** no puede aprender la dirección MAC de **ecs01** cuando se usa la dirección IP privada para hacer ping a **ecs01**.
3. Ejecute el comando **ip a** en **ecs01** para comprobar la configuración de NIC de **ecs01**. La siguiente figura muestra un ejemplo.

Figura 8-1 Consulta de la configuración de NIC de **ecs01**

```
[root@bd-slave1 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:62:1d:d5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.141/24 brd 192.168.1.255 scope global eth0
    inet 192.168.1.40/32 scope global eth0
    inet6 fe80::f816:3eff:fe62:1dd5/64 scope link
        valid_lft forever preferred_lft forever
```

La dirección IP 192.168.1.40/32 no debe configurarse en función de la salida del comando. Como resultado, **ecs01** no puede enviar paquetes a **ecs02**.

Procedimiento

Modifique la configuración de NIC de **ecs01**. Ejecute el comando siguiente para eliminar la dirección IP redundante, por ejemplo, 192.168.1.40/32, configurada en la NIC **eth0**:

ip a del 192.168.1.40/32 dev eth0

8.6 ¿Por qué falla la comunicación entre dos ECS en la misma VPC o ocurre una pérdida de paquetes cuando se comunican?

Síntoma

Dos ECS en la misma VPC no pueden comunicarse entre sí o hay pérdida de paquetes cuando se comunican.

Resolución de problemas

Los problemas aquí se describen en orden de la probabilidad de que ocurran.

Solucione el problema descartando las causas descritas aquí, una por una.

Figura 8-2 Resolución de problemas

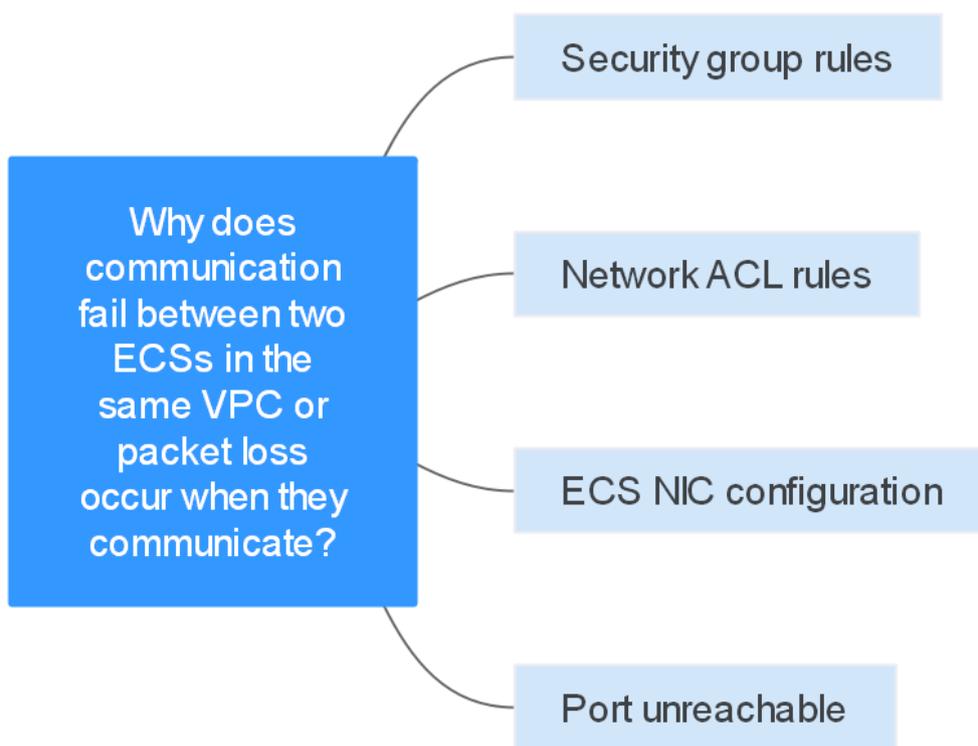


Tabla 8-1 Resolución de problemas

Causa posible	Solución
Reglas de grupos de seguridad	Consulte Reglas de grupos de seguridad
Reglas de ACL de red	Consulte Reglas de ACL de red

Causa posible	Solución
Configuración de NIC de ECS	Consulte Configuración de NIC de ECS
Puerto inalcanzable	Consulte Puerto inalcanzable

Reglas de grupos de seguridad

Compruebe si el grupo de seguridad NIC de ECS permite el tráfico ICMP saliente y entrante.

Tome la dirección de entrada como ejemplo. Las reglas del grupo de seguridad deben contener al menos una de las siguientes reglas.

Figura 8-3 Regla de grupo de seguridad entrante

<input type="checkbox"/> Protocol & Port ▼ ?	Type	Source ?	Description	Operation
<input type="checkbox"/> All	IPv4	0.0.0.0/0 ?	--	Modify Replicate Delete
<input type="checkbox"/> ICMP: All	IPv4	0.0.0.0/0 ?	--	Modify Replicate Delete

Si se prueban paquetes de otros protocolos, configure las reglas de grupo de seguridad para permitir el tráfico de protocolo correspondiente. Por ejemplo, si se prueban los paquetes de UDP, compruebe si el grupo de seguridad permite el tráfico UDP entrante.

Reglas de ACL de red

1. Compruebe si la subred de la NIC de ECS tiene una ACL de red asociada.
2. Compruebe el estado de la ACL de la red en la lista de ACL de la red.
 - Si se muestra **Disabled** en la columna **Status**, se ha deshabilitado la ACL de red. Vaya a [3](#).
 - Si se muestra **Enabled** en la columna **Status**, se ha habilitado la ACL de red. Vaya a [4](#).
3. Haga clic en el nombre de la ACL de la red y configure las reglas en las fichas **Inbound Rules** y **Outbound Rules** para permitir el tráfico ICMP.
4. Si la ACL de red está deshabilitada, todos los paquetes en las direcciones entrantes y salientes se descartan de forma predeterminada. En este caso, elimine la ACL de red o habilite la ACL de red y permita el tráfico ICMP.

Configuración de NIC de ECS

El siguiente procedimiento utiliza un ECS de Linux como ejemplo. Para un ECS de Windows, compruebe las restricciones del firewall.

1. Compruebe si varias NIC están configuradas para el ECS. Si el ECS tiene varias NIC y una EIP está enlazada a una NIC de extensión, configure el enrutamiento basado en políticas para el ECS. Para más detalles, consulte [¿Cómo configuro las rutas basadas en políticas para un ECS con varias NIC?](#)
2. Inicie sesión en el ECS y ejecute el siguiente comando para comprobar si la NIC se ha creado y obtenido una dirección IP privada. Si no hay información de NIC o no se puede obtener la dirección IP privada, póngase en contacto con el soporte técnico.

ifconfig

Figura 8-4 Dirección IP de NIC

```
root@ecs-acl ~# ifconfig
eth0 Link encap:Ethernet HWaddr FA:16:3E:BC:B7:81
      inet addr:192.168.72.289 Bcast:192.168.72.255 Mask:255.255.255.0
      inet6 addr: fe80::f816:3eff:febc:b781/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:881 errors:0 dropped:0 overruns:0 frame:0
      TX packets:547 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:49684 (48.4 KiB) TX bytes:44454 (43.4 KiB)
      Interrupt:46
```

3. Si el uso de la CPU supera el 80%, la comunicación de ECS puede verse afectada negativamente. Ejecute el siguiente comando para comprobar si el uso de CPU del ECS es demasiado alto:

top

4. Ejecute el siguiente comando para comprobar si el ECS tiene alguna restricción en las reglas del grupo de seguridad:

iptables-save

5. Ejecute el siguiente comando para comprobar si el archivo `/etc/hosts.deny` contiene las direcciones IP que limitan la comunicación:

vi /etc/hosts.deny

Si el archivo `hosts.deny` contiene la dirección IP de otro ECS, elimine la dirección IP del archivo `hosts.deny` y guarde el archivo.

Puerto inalcanzable

1. Si no se puede alcanzar un puerto del ECS, compruebe si las reglas de grupo de seguridad y las reglas de ACL de red habilitan el puerto.
2. En el ECS de Linux, ejecute el siguiente comando para comprobar si el ECS escucha en el puerto: Si el ECS no escucha en el puerto, la comunicación del ECS puede verse afectada negativamente.

`netstat -na | grep <Port number>`

Envío de un ticket de servicio

Si el problema persiste, [envíe un ticket de servicio](#).

8.7 ¿Por qué mi ECS no puede usar Cloud-init?

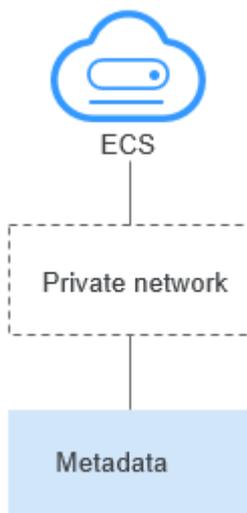
Síntomas

Un ECS no puede usar cloud-init.

Resolución de problemas

[Figura 8-5](#) muestra el proceso para que un ECS obtenga metadatos usando el cloud-init.

Figura 8-5 Proceso de obtención de metadatos



Compruebe las siguientes causas posibles.

Figura 8-6 Causas posibles

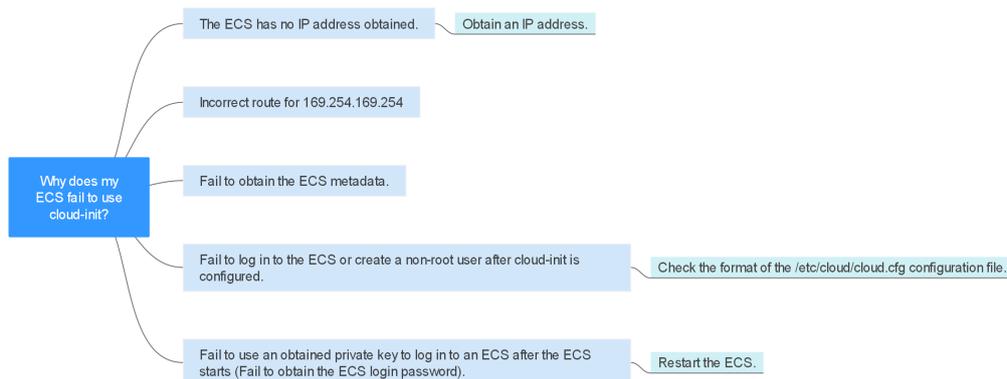


Tabla 8-2 Causas posibles

Causa posible	Solución
El ECS no tiene ninguna dirección IP obtenida.	Consulte El ECS no ha obtenido la dirección IP
Ruta incorrecta para 169.254.169.254	Consulte Ruta incorrecta para 169.254.169.254
Error al obtener los metadatos de ECS.	Consulte No obtuvo los metadatos de ECS
No se puede iniciar sesión en el ECS o crear un usuario no root después de configurar Cloud-init.	Compruebe el formato del archivo de configuración <code>/etc/cloud/cloud.cfg</code> . Para obtener más información, véase No se puede iniciar sesión en ECS o crear un usuario que no sea root después de que cloud-init esté configurado.

Causa posible	Solución
No se puede utilizar una clave privada obtenida para iniciar sesión en un ECS después de que se inicie el ECS (no se puede obtener la contraseña de inicio de sesión de ECS).	Reinicie el ECS e inténtelo de nuevo.

El ECS no ha obtenido la dirección IP

Compruebe si el ECS ha obtenido una dirección IP.

Si no se obtiene ninguna dirección IP, ejecute el comando **dhclient** para obtener la dirección IP (este comando varía dependiendo de los SO de ECS). Alternativamente, puede ejecutar el comando **ifdown ethx** para deshabilitar el puerto de red y, a continuación, ejecutar el comando **ifup ethx** para habilitarlo para permitir que la NIC de ECS obtenga automáticamente una dirección IP de nuevo.

Figura 8-7 Dirección IP del ECS

```
-bash-4.1# ifconfig
eth0      Link encap:Ethernet  HWaddr FA:16:3E:BD:36:DD
          inet addr:192.168.1.200  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:febd:36dd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:73008 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26295 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4162713 (3.9 MiB)  TX bytes:2336476 (2.2 MiB)
          Interrupt:35

eth1      Link encap:Ethernet  HWaddr FA:16:3E:A9:C7:1D
          inet addr:192.168.1.179  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fea9:c71d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45026 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12244 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1270534 (1.2 MiB)  TX bytes:4178924 (3.9 MiB)
          Interrupt:34

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:28 (28.0 b)  TX bytes:28 (28.0 b)
```

Ruta incorrecta para 169.254.169.254

Haga ping a **169.254.169.254/32** desde el ECS. Si la dirección IP no se puede hacer ping, realice los siguientes pasos:

1. Compruebe la ruta exacta configurada en el ECS para la dirección IP **169.254.169.254/32**.

En la mayoría de los casos, el salto siguiente de la ruta exacta para la dirección IP **169.254.169.254/32** es el mismo que el de la ruta predeterminada para la dirección IP.

Figura 8-8 Ruta para la dirección IP **169.254.169.254/32**

```
-bash-4.1# ip route
169.254.169.254 via 192.168.1.1 dev eth0 proto static
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.200
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.179
169.254.0.0/16 dev eth0 scope link metric 1002
default via 192.168.1.1 dev eth0 proto static
-bash-4.1#
```

2. Si no hay una ruta exacta para la dirección IP **169.254.169.254/32**, la causa es la siguiente:
Las imágenes con el SO de CentOS 5 no son compatibles con cloud-init. Para usar cloud-init, seleccione un SO diferente.
3. Si el salto siguiente de la ruta exacta para la dirección IP **169.254.169.254/32** es diferente de la ruta predeterminada para la dirección IP:
 - Si el ECS se creó antes de que se habilitara cloud-init, ejecute **service network restart** para obtener la ruta correcta.
 - Si el ECS se ha creado recientemente, **envíe un ticket de servicio** o póngase en contacto con el soporte técnico.

No obtuvo los metadatos de ECS

Ejecute el siguiente comando en el ECS para obtener los metadatos:

```
curl http://169.254.169.254/openstack/latest/meta_data.json
```

Si se muestra información similar a la mostrada en **Figura 8-9**, el ECS obtiene con éxito los metadatos.

Figura 8-9 Resultado de comandos

```
-bash-4.1# curl http://169.254.169.254/openstack/latest/meta_data.json
{"random_seed": "rTUsD1EH6A jUKLnvg51U8S0pH6xC78MFRTeW10munBNyqos6q/EsAEJondF8iJkMDG0TzbCTbB15HntS9X
XHu61u+y8fAeylkaA j60A08KHPGdv6Xdf hku6qu jCr jXn5hUFvqfZ/yaJ3LrAE jB8N j59hI +wmbP i8oYc2WzYmTqWjXYRNwpmqJM
sIKYm0CLdFbwYoZaK lY27/WEUZDU0Q1GpRkkuNwfaCN/rQQ/hHd+3UuSJbArsgUeoWCTp5oxixLiCJzSSHARz41UiZiRauYwm0go
iTFtopvZTwmYEk lFmkZsy7h6PP0kgm jgPn+1kZf0qgJht lVpyBr2pw4aPAeZa4z7QX1Rtmt7MlyGUbea85/1PDUE1J/GJpoH1/+z
rDye lA09Cs0G1UFuELadyDer4k4k42f0o7dDmEjDm lNnE8eega5r7Eohb04RTimzi +3nb10Q jPq/S7J +mFM/UoZEJH0bZE4uWlAj
Znhvy/pc6ho7fQKbX0C78f biPh59CKyF0W835nNJ/CZNNBtd3UdG25SQ701FnA+NtbDeo8+g05iFLweww0G5BLC jm1f jh9 +mqot
+5ae6ZceXds l1fscqmb jwCnCimthJlYGmbxu+6Fm9XpLDopDfrREBUcRSnt IK67JprBSRppc+4sMygiuKYlJ0TUJYQYDBUzB7F3o
=", "uuid": "53ebb737-ddc5-4303-9fac-aa72b00b101a", "availability_zone": "eu-de-02", "hostname": "ec
s-gjm-55eb.novalocal", "launch_index": 0, "meta": {"metering.image_id": "98721f93-722f-4386-a975-3cb
df1abf56d", "metering.imagetype": "gold", "metering.resourcespeccode": "c2.large.oracle", "metering.
cloudServiceType": "sys.service.type.ec2", "image_name": "AutoC_DTC_OEL_6.8", "metering.resourcetype
": "1", "os_bit": "64", "opc_id": "420b71c7-94ac-45b8-8ed6-30aafc8fbdba", "os_type": "Linux", "charg
ing_mode": "0"}, "project_id": "efdf974f549b4eaab85c3903ddd2ab0e", "name": "ecs-gjm-55eb"}-bash-4.1#
```

No se puede iniciar sesión en ECS o crear un usuario que no sea root después de que cloud-init esté configurado

Compruebe si el formato del archivo de configuración **/etc/cloud/cloud.cfg** es correcto. Para obtener más información, consulte los requisitos de formato de archivo para diferentes distribuciones de Linux. La siguiente figura muestra un ejemplo de archivo de configuración **/etc/cloud/cloud.cfg** para Ubuntu.

Figura 8-10 Archivo de configuración

```
system_info:
# This will affect which distro class gets used
distro: rhel
# Default user name + that default users groups (if added/used)
default_user:
  name: linux // Specifies the username for login.
  lock_passwd: False // The value False indicates that the password login mode is enabled. For some OSs, the value 0 indicates that the password login mode is enabled.
gecos: Cloud User
groups: users // Specifies whether the user will be added to a group. This parameter is optional. The groups parameter value must be an existing group under /etc/group in the system.
passwd: $6$I63DBVKK$Zh4lchiJR7NuZvtJH5YBQJlg5RoQCRL5IX2H5g j25JwXITKU01we8WYcwbze aS2VWpRmNo28vaxxCyU6LwoD0
sudo: ["ALL=(ALL) NOPASSWD:ALL"] // Specifies that all permissions of user root will be granted to the user.
shell: /bin/bash // Specifies that the bash shell is used.
# Other config here will be given to the distro class and/or path classes
paths:
  cloud_dir: /var/lib/cloud/
  templates_dir: /etc/cloud/templates/
ssh_svcname: sshd
```

La clave privada obtenida no se puede usar para iniciar sesión en un ECS después de que se inicie el ECS (no se pudo obtener la contraseña de inicio de sesión de ECS)

Reinicie el ECS para rectificar la falla.

Envío de un ticket de servicio

Si el EIP aún no puede usar cloud-init después de realizar los pasos anteriores, [envíe un ticket de servicio](#).

Proporcione la siguiente información al ingeniero de soporte técnico.

Concepto	Descripción	Ejemplo	Valor
Bloque CIDR de VPC	Requerido para la configuración de gateway de clientes	Ejemplo: 10.0.0.0/16	N/A
ID de la VPC	N/A	Ejemplo: 120b71c7-94ac-45b8-8ed6-30aafc8fbdba	N/A
Bloque CIDR de la subred 1 (puede ser el mismo que el bloque CIDR de VPC)	N/A	Ejemplo: 10.0.1.0/24	N/A
ID del ECS	N/A	N/A	N/A
Dirección IP del ECS	N/A	Ejemplo: 192.168.1.192/24	N/A
Información de ruta del ECS	N/A	N/A	-

8.8 ¿Por qué mi ECS no puede acceder a Internet incluso después de que una EIP está vinculada?

Síntomas

Un ECS con una EIP enlazada no puede acceder a Internet.

Resolución de problemas

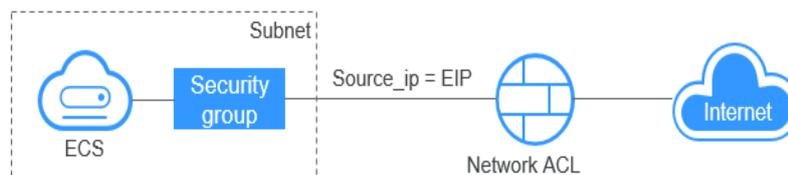
Comprobación de si las EIP están bloqueadas o congeladas

- Compruebe si la EIP está bloqueada. Para obtener más información, consulte [¿Cómo desbloqueo una EIP?](#)
- Compruebe si la EIP está congelada. Para obtener más información, consulte [¿Por qué mis EIP están congeladas? ¿Cómo descongelo mis EIP?](#)

Comprobación de la conectividad de EIP

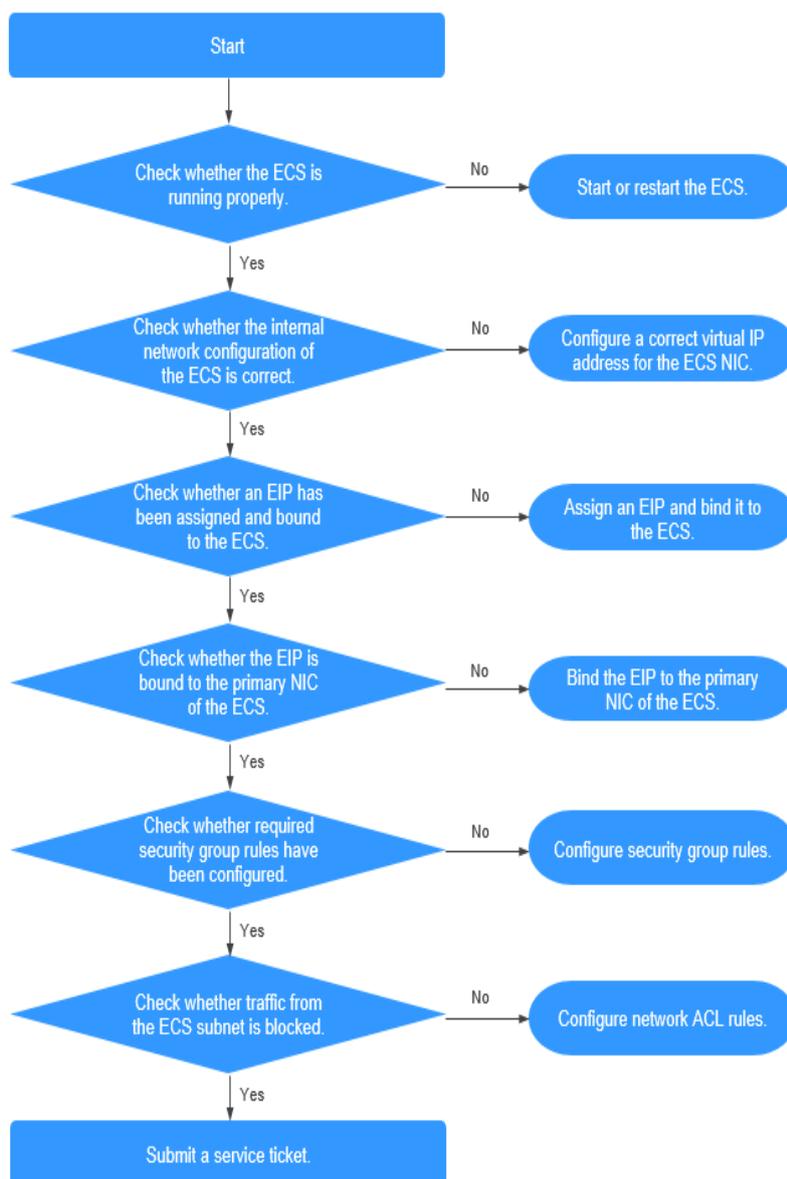
Figura 8-11 muestra el diagrama de red para que un ECS acceda a Internet por una EIP.

Figura 8-11 Diagrama de red de EIP



Localice la falla según el siguiente procedimiento.

Figura 8-12 Procedimiento de resolución de problemas



1. **Paso 1: Compruebe si el ECS está funcionando correctamente**
2. **Paso 2: Compruebe si la configuración de red del ECS es correcta**
3. **Paso 3: Compruebe si una EIP ha sido asignada y vinculada al ECS**
4. **Paso 4: Compruebe si una EIP está vinculada a la NIC primaria del ECS**
5. **Paso 5: Compruebe si se han configurado las reglas de grupo de seguridad requeridas.**
6. **Paso 6: Compruebe si el tráfico de la subred del ECS está bloqueado**

Paso 1: Compruebe si el ECS está funcionando correctamente

Compruebe el estado del ECS.

Si el estado del ECS no es **Running**, inicie o reinicie el ECS.

Figura 8-13 Estado de ECS

Name ID	AZ	Status	Specifications/Image	Private IP Address	EIP	Operation
ecs-gm-ff56c 5386b731-6dc5-4300-9fac-aa7200a	eu-central-2	Running	2 vCPUs 4 GB AutoC_OTC_OEL_6.8	192.168.1.200	-	Remote Login More +

Paso 2: Compruebe si la configuración de red del ECS es correcta

1. Compruebe si la NIC del ECS tiene una dirección IP asignada.
 Inicie sesión en el ECS y ejecute `ifconfig` o `ip address` para comprobar la dirección IP de la NIC de ECS.
 Si tanto la NIC principal como la de extensión de un ECS tienen una EIP vinculada, compruebe si el ECS tiene rutas basadas en políticas configuradas. Si las rutas basadas en políticas no están configuradas, consulte [Configuración de las rutas basadas en políticas para un ECS de Linux con varias NIC \(IPv4/IPv6\)](#).
 Si el ECS ejecuta Windows, ejecute `ipconfig`.
2. Compruebe si la NIC de ECS tiene una dirección IP virtual.
 Inicie sesión en ECS y ejecute `ifconfig` o `ip address` para comprobar si la NIC de ECS tiene una dirección IP virtual. Si la NIC de ECS no tiene una dirección IP virtual, ejecute el comando `ip addr add virtual IP address eth0` para configurar una dirección IP para la NIC de ECS.

Figura 8-14 Dirección IP virtual de una NIC

```
[root@demoserver ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether fa:16:3e:37:7b:62 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.30/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 84950sec preferred_lft 84950sec
    inet 192.168.1.192/24 scope global secondary eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe37:7b62/64 scope link
        valid_lft forever preferred_lft forever
```

Compruebe si la NIC de ECS tiene una ruta predeterminada. Si no hay una ruta predeterminada, ejecute `ip route add` para agregar una.

Figura 8-15 Ruta predeterminada

```
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.200
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.179
169.254.0.0/16 dev eth0 scope link metric 1002
default via 192.168.1.1 dev eth0 proto static
-bash-4.1#
```

Paso 3: Compruebe si una EIP ha sido asignada y vinculada al ECS

Comprobar si una EIP ha sido asignada y vinculada al ECS. Si no se ha asignado ninguna EIP, asigne una EIP y vincule a la ECS.

El ECS mostrado en [Figura 8-16](#) no tiene límite de EIP. Solo tiene una dirección IP privada enlazada.

Figura 8-16 Estado de la EIP

Name/ID	Monitoring	AZ	Status	Specifications/Image	IP Address
ecs- c93dd6d2-9774-4828-98a2-486c0466cb51		AZ1	Running	4 vCPUs 8 GB c6.xlarge.2 Windows Server 2016 Standard ...	192.168.0.146 (Private IP)

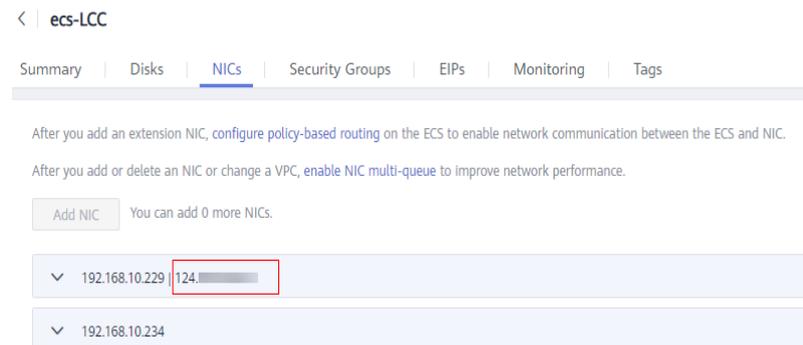
Paso 4: Compruebe si una EIP está vinculada a la NIC primaria del ECS

Compruebe si una EIP está vinculada a la NIC principal del ECS. Si no hay ninguna EIP unida a la NIC principal del ECS, vincule una.

Puede ver los detalles de la NIC haciendo clic en la ficha **NICs** de la página de detalles del ECS. De forma predeterminada, el primer registro de la lista es la NIC principal.

Como se muestra en **Figura 8-17**, la EIP está unida a la NIC primaria.

Figura 8-17 Comprobación de si la EIP está vinculada a la NIC primaria del ECS



Paso 5: Compruebe si se han configurado las reglas de grupo de seguridad requeridas.

Para obtener más información acerca de cómo agregar reglas de grupo de seguridad, consulte la [Adición de una regla de grupo de seguridad](#).

Si no se han configurado las reglas de grupo de seguridad, configúrelas en función de los requisitos de servicio. (La dirección IP remota indica la dirección IP permitida y **0.0.0.0/0** indica que todas las direcciones IP están permitidas.)

Paso 6: Compruebe si el tráfico de la subred del ECS está bloqueado

Compruebe si el ACL de red de la subred NIC bloquea cierto tráfico de la subred.

Puede configurar el ACL de red en la consola de VPC. Asegúrese de que las reglas de ACL de red permiten el tráfico de la subred del ECS.

8.9 ¿Cómo manejo un fallo de red del IB?

Fallo de comunicación de RDMA entre dos ECS de IB

1. Compruebe si las claves en los dos ECS son consistentes.

Ejecute el siguiente comando para comprobar las claves asignadas a los ECS:

```
cat /sys/class/infiniband/mlx5_0/ports/1/pkeys/* | grep -v "0x0000"
```

Figura 8-18 Comprobación de la coherencia de Pkey

```
[root@test2 ~]# cat /sys/class/infiniband/mlx5_0/ports/1/pkeys/* | grep -v "0x0000"  
0x8ee5  
0x7fff
```

- Si solo se obtiene una clave, póngase en contacto con el soporte técnico.
 - Si se obtienen dos Pkeys, asegúrese de que las dos Pkeys en los dos ECSs son iguales.
2. Ejecute el siguiente comando para comprobar si el firewall está deshabilitado:
- service firewalld status**

Figura 8-19 Comprobación del firewall

```
[root@test2 ~]# service firewalld status
Redirecting to /bin/systemctl status firewalld.service
• firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: inactive (dead) since Tue 2018-01-02 20:27:36 EST; 10h ago
    Docs: man:firewalld(1)
   Process: 861 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)
  Main PID: 861 (code=exited, status=0/SUCCESS)

Jan 02 06:04:39 ecs-g00200264-h2-0002.novalocal systemd[1]: Starting firewalld - dynamic firewall daemon...
Jan 02 06:04:39 ecs-g00200264-h2-0002.novalocal systemd[1]: Started firewalld - dynamic firewall daemon.
Jan 02 20:27:35 test2 systemd[1]: Stopping firewalld - dynamic firewall daemon...
Jan 02 20:27:36 test2 systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

Si el firewall no está deshabilitado, ejecute el siguiente comando para deshabilitarlo:

service firewalld stop

3. Compruebe si el comando de comunicación RDMA es correcto.

Ejecute el siguiente comando en ECS 1 (cliente):

ib_write_lat -x 0 --pkey_index 0 192.168.0.218

Ejecute el siguiente comando en ECS 2 (servidor):

ib_write_lat -x 0 --pkey_index 0

Sin dirección IP para el puerto IB de ECS

Si ejecuta **ifconfig** y el resultado del comando muestra que no se ha asignado ninguna dirección IP al puerto de InfiniBand ECS (IB):

1. Ejecute el siguiente comando para comprobar la clave:

cat /sys/class/infiniband/mlx5_0/ports/1/pkeys/* | grep -v "0x0000"

Figura 8-20 Comprobando Pkey

```
[root@test2 ~]# cat /sys/class/infiniband/mlx5_0/ports/1/pkeys/* | grep -v "0x0000"
0x8ee5
0x7fff
```

Si solo se obtiene una clave, póngase en contacto con el soporte técnico.

2. Ejecute el siguiente comando para asignar una dirección IP al puerto ECS IB:

dhclient ib0

Si no se muestra ningún resultado del comando, la dirección IP no se puede obtener mediante DHCP.

3. Póngase en contacto con el servicio de asistencia técnica.

Después de haber realizado los pasos anteriores, si la red del IB aún no se puede utilizar para la comunicación o el puerto del IB aún no puede obtener una dirección IP, póngase en contacto con el servicio de asistencia técnica para obtener asistencia y proporcione al ingeniero de asistencia técnica la siguiente información.

Artículo	Descripción	Ejemplo	Valor
VP C1 ID	ID de VPC 1	Ejemplo: fef65559-c154-4229-afc4-9ad0314437ea	N/A
VM 1 ID	ID de ECS 1 en VPC 1	Ejemplo: f7619b12-3683-4203-9271-f34f283cd740	N/A
VM 2 ID	ID de ECS 2 en VPC 1	Ejemplo: f75df766-68aa-4ef3-a493-06cdc26ac37a	N/A

8.10 ¿Por qué mi ECS no puede comunicarse en una red de nivel 2 o 3?

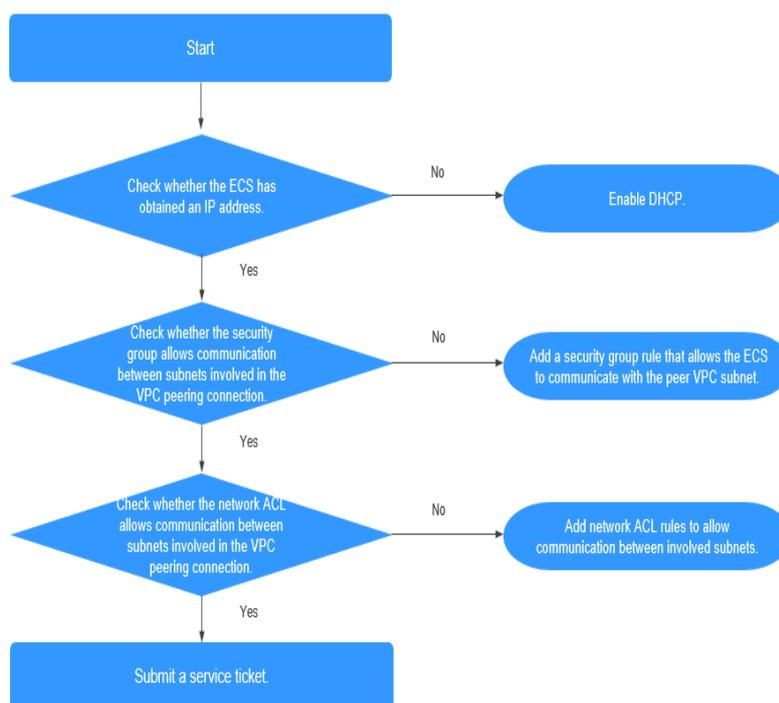
Síntoma

Un ECS no puede hacer ping al gateway de la subred donde reside el ECS.

Resolución de problemas

Localice el fallo basado en el siguiente procedimiento.

Figura 8-21 Procedimiento de resolución de problemas



1. [Comprobación de si el ECS ha obtenido una dirección IP](#)
2. [Comprobación de si el grupo de seguridad permite la comunicación entre subredes involucradas en la interconexión de VPC](#)
3. [Comprobación de si la ACL de red permite la comunicación entre subredes involucradas en la interconexión VPC](#)

Comprobación de si el ECS ha obtenido una dirección IP

Inicie sesión en el ECS y ejecute **ifconfig** o **ip address** para comprobar la dirección IP de la NIC de ECS. Si un ECS ejecuta Windows, utilice **ipconfig**.

Si el ECS no tiene una dirección IP, compruebe si DHCP se ha habilitado para la subred requerida.

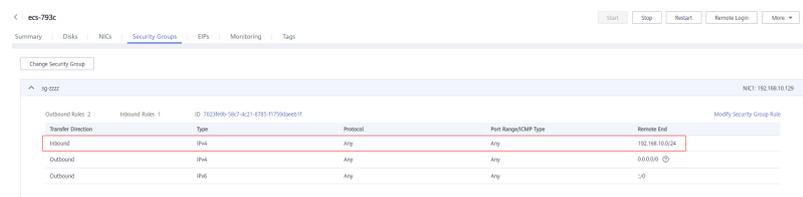
Cambie a la página de detalles de subred y compruebe si se ha habilitado la función DHCP.

Para más detalles, consulte [¿Por qué mi ECS no puede obtener una dirección IP?](#)

Comprobación de si el grupo de seguridad permite la comunicación entre subredes involucradas en la interconexión de VPC

Puede ver el grupo de seguridad en la página de detalles de ECS. Compruebe si se ha configurado una regla de grupo de seguridad para permitir que el ECS se comunique con la subred VPC del mismo nivel.

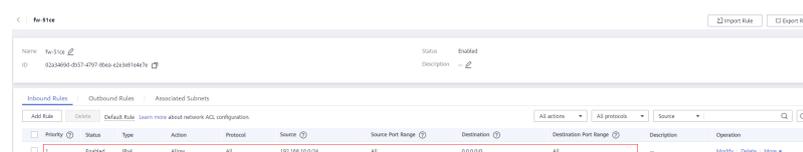
Figura 8-22 Regla del grupo de seguridad



Comprobación de si la ACL de red permite la comunicación entre subredes involucradas en la interconexión VPC

En el panel de navegación de la izquierda de la consola de VPC, elija **Network ACLs**. En la página mostrada, seleccione la ACL de red asociada a las subredes de la interconexión de VPC. En la página de detalles de ACL de red, compruebe si las reglas de ACL de red permiten la comunicación entre las subredes implicadas en la interconexión de VPC.

Figura 8-23 Regla de ACL de red



Envío de un ticket de servicio

Si el problema persiste, [envíe un ticket de servicio](#).

8.11 ¿Cómo manejo un fallo de red BMS?

1. Ejecute el siguiente comando para comprobar si los puertos de red BMS se han unido:

ifconfig

Figura 8-24 Comprobación de la fianza

```
[root@bms2 rhel]# ifconfig
bond0    Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
         inet addr:192.168.2.46  Bcast:192.168.2.255  Mask:255.255.255.0
         inet6 addr: fe80::f816:3eff:fee9:b08a/64 Scope:Link
         UP BROADCAST RUNNING PROMISC MASTER MULTICAST  MTU:8888  Metric:1
         RX packets:188108 errors:0 dropped:0 overruns:0 frame:0
         TX packets:112119 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:42689694 (40.7 MiB)  TX bytes:82939564 (79.0 MiB)

bond0.2966 Link encap:Ethernet  HWaddr FA:16:3E:60:9C:CF
         inet addr:192.168.4.113  Bcast:192.168.4.255  Mask:255.255.255.0
         inet6 addr: fe80::f816:3eff:fe60:9ccf/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:8888  Metric:1
         RX packets:12 errors:0 dropped:0 overruns:0 frame:0
         TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:660 (660.0 b)  TX bytes:720 (720.0 b)

eth0     Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
         UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
         RX packets:174667 errors:0 dropped:0 overruns:0 frame:0
         TX packets:112119 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:41874228 (39.9 MiB)  TX bytes:82939564 (79.0 MiB)

eth1     Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
         UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
         RX packets:13441 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:815466 (796.3 KiB)  TX bytes:0 (0.0 b)
```

Si no se obtiene información de unión, los puertos de red de BMS no están unidos. Póngase en contacto con el servicio de asistencia técnica.

2. Ejecute el siguiente comando para comprobar si la información de ruta de BMS es correcta:

route -n

Figura 8-25 Comprobación de la información de ruta de BMS

```
[root@bms2 rhel]# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
169.254.169.254 192.168.2.1 255.255.255.255 UGH 0 0 0 bond0
192.168.4.0 0.0.0.0 255.255.255.0 U 0 0 0 bond0.2966
192.168.2.0 0.0.0.0 255.255.255.0 U 0 0 0 bond0
169.254.0.0 0.0.0.0 255.255.0.0 U 1006 0 0 bond0
169.254.0.0 0.0.0.0 255.255.0.0 U 1007 0 0 bond0.2966
0.0.0.0 192.168.2.1 0.0.0.0 UG 0 0 0 bond0
[root@bms2 rhel]# █
```

Compruebe si existe la ruta predeterminada (con un destino de 0.0.0.0/0).

Figura 8-26 Comprobación de la ruta predeterminada

```
0.0.0.0 192.168.2.1 0.0.0.0 UG 0 0 0 bond0
[root@bms2 rhel]# █
```

Compruebe si existe una ruta a 169.254.169.254.

Figura 8-27 Comprobación de la ruta para el rango de direcciones IP 169.254.169.254

```
Destination Gateway Genmask Flags Metric Ref Use Iface
169.254.169.254 192.168.2.1 255.255.255.255 UGH 0 0 0 bond0
```

Si las rutas requeridas no están allí, póngase en contacto con el soporte técnico.

3. Si los BMS de una VPC no pueden comunicarse entre sí o un BMS con un enlace de EIP no puede acceder a Internet, rectifique el fallo basándose en las preguntas frecuentes relacionadas.
4. Si el error no se puede corregir después de realizar estas operaciones, póngase en contacto con el soporte técnico.

Obtenga la información de VPC y BMS en la consola de gestión y proporcione al ingeniero de soporte técnico la siguiente información.

Artículo	Descripción	Ejemplo	Valor
VPC 1 ID	ID de VPC 1	Ejemplo: fef65559-c154-4229-afc4-9ad0314437ea	N/A
BMS 1 ID	ID de BMS 1 en VPC 1	Ejemplo: f7619b12-3683-4203-9271-f34f283cd740	N/A
BMS 2 ID	ID de BMS 2 en VPC 1	Ejemplo: f75df766-68aa-4ef3-a493-06cdc26ac37a	N/A

8.12 ¿Por qué mi ECS no puede obtener una dirección IP?

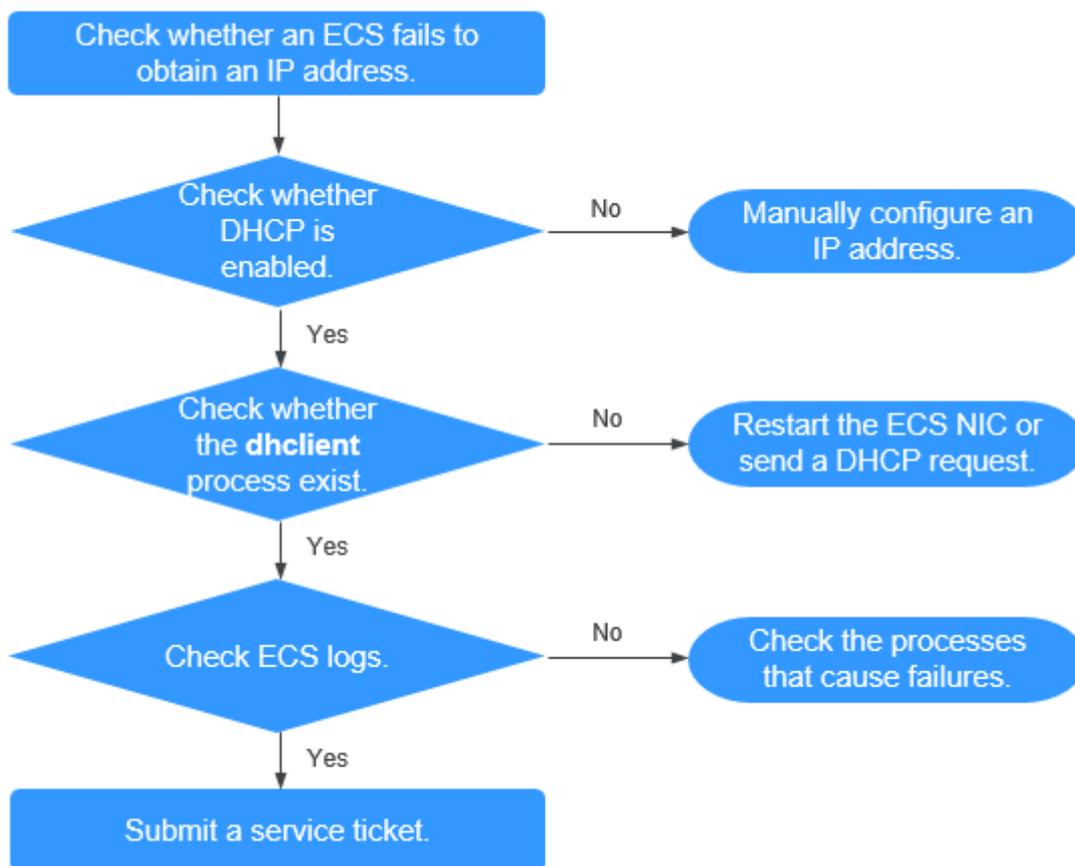
Síntoma

La dirección IP privada del ECS no se obtiene.

Resolución de problemas

Localice el fallo basado en el siguiente procedimiento.

Figura 8-28 Proceso de solución de problemas



1. **Comprobación de si DHCP está habilitado**
2. **Comprobación de si existe el proceso dhclient**
3. **Comprobación de logs de ECS**

Comprobación de si DHCP está habilitado

Compruebe si la función de DHCP de la subred está habilitada (habilitada de forma predeterminada).

Cambie a la página de detalles de subred. Si DHCP está deshabilitado, debe configurar manualmente una dirección IP estática para el ECS haciendo referencia al paso 3.

Comprobación de si existe el proceso dhclient

1. Compruebe si el proceso **dhclient** existe:
ps -ef | grep dhclient
2. Si el proceso **dhclient** no existe, inicie sesión en el ECS y reinicie la NIC de ECS o envíe una solicitud DHCP.
 - Linux:
Ejecute el comando **dhclient ethx**. Si se admiten comandos **dhclient**, ejecute el comando **ifdown ethx;ifup ethx**. En el comando, *ethx* indica la NIC de ECS, por ejemplo, **eth0** y **eth1**.

- Windows:
Desconecte la conexión de red y conéctela.
- 3. Si el cliente DHCP no envía las solicitudes durante mucho tiempo, por ejemplo, el error se produce de nuevo después de reiniciar la NIC, puede utilizar el siguiente método para configurar la dirección IP estática.
 - Linux:
 - i. Ejecute el siguiente comando para abrir el archivo `/etc/sysconfig/network-scripts/ifcfg-eth0`:
vi /etc/sysconfig/network-scripts/ifcfg-eth0
 - ii. Modifique los siguientes elementos de configuración en el archivo `/etc/sysconfig/network-scripts/ifcfg-eth0`.
BOOTPROTO=static
IPADDR=192.168.1.100 #IP address
NETMASK=255.255.255.0 #Subnet mask
GATEWAY=192.168.1.1 #Gateway address
 - iii. Ejecute el siguiente comando para reiniciar el servicio de red:
service network restart
 - Windows:
En la ficha **Local Area Connection Status**, haga clic en **Properties**. En el área que se muestra, seleccione **Internet Protocol Version 4 (TCP/IPv4)** y haga clic en **Properties**. En el área que se muestra, introduzca la dirección IP, la máscara de subred y la dirección del gateway predeterminada.

Comprobación de logs de ECS

Compruebe el log de **messages** de ECS en el directorio `/var/log/messages`.

Busque la dirección MAC de la NIC y compruebe si hay algún proceso que cause fallas en la obtención de direcciones IP a través de DHCP.

Envío de un ticket de servicio

Si el problema persiste, [envíe un ticket de servicio](#).

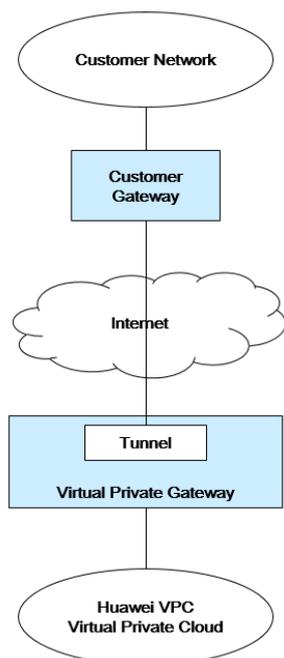
Proporcione al servicio de atención al cliente el ID de ECS, el ID de la subred utilizada por el ECS y el ID de la VPC utilizada por el ECS.

8.13 ¿Cómo manejo un fallo de red de conexión directa o VPN?

Red de VPN

[Figura 8-29](#) muestra su red, el gateway del cliente, la VPN y la VPC.

Figura 8-29 Red de VPN



Guía de autoverificación del cliente

1. Proporcione la información de su red.

Obtener información listada en **Tabla 8-3**. Esta tabla muestra valores de ejemplo. Puede determinar los valores reales basándose en los valores de ejemplo. Debe obtener todos los valores reales de su proyecto.

📖 NOTA

Puede imprimir esta tabla y completar sus valores.

Tabla 8-3 Información de la red

Artículo	Descripción	Ejemplo	Valor
VPC CIDR block	Requerido para la configuración de gateway de clientes	Ejemplo: 10.0.0.0/16	N/A
VPC ID	N/A	N/A	N/A
CIDR block of subnet 1 (can be the same as the VPC CIDR block)	N/A	Ejemplo: 10.0.1.0/24	N/A
ECS ID	N/A	N/A	N/A
Customer gateway type (for example, Cisco)	N/A	N/A	N/A

Artículo	Descripción	Ejemplo	Valor
Public IP address used by the customer gateway	N/A	El valor debe ser estático.	N/A

2. Proporcione la información de configuración del gateway.

Puede comprobar los problemas de conectividad del gateway en función de los siguientes pasos:

Debe tener en cuenta IKE, IPsec, reglas de ACL y la selección de ruta. Puede rectificar el fallo en cualquier secuencia que desee. Sin embargo, se recomienda que compruebe el error en la siguiente secuencia: IKE, IPsec, reglas de ACL y selección de ruta.

- a. Obtenga la política de IKE utilizada por el dispositivo del gateway.
- b. Obtenga la política de IPsec utilizada por el dispositivo del gateway.
- c. Obtenga la regla de ACL utilizada por su dispositivo del gateway.
- d. Compruebe si su dispositivo del gateway puede comunicarse con los dispositivos del gateway en la nube.

 **NOTA**

Los comandos utilizados en los diferentes dispositivos de gateway son diferentes. Puede ejecutar los comandos basados en su dispositivo de gateway (como los dispositivos de Cisco, de H3C, de AR o de Fortinet) para obtener la información requerida anterior.

Operaciones O&M que requieren asistencia

Debe enviar solicitudes de comunicación desde los ECS al dispositivo remoto.

Método:

Inicie sesión en un ECS y haga ping a una dirección IP en su centro de datos local.

8.14 ¿Por qué se puede acceder a mi servidor desde Internet pero no puede acceder a Internet?

Síntoma

Se puede acceder al servidor desde, pero no puede acceder a Internet.

Resolución de problemas

Compruebe las siguientes causas posibles.

Figura 8-30 Causas posibles

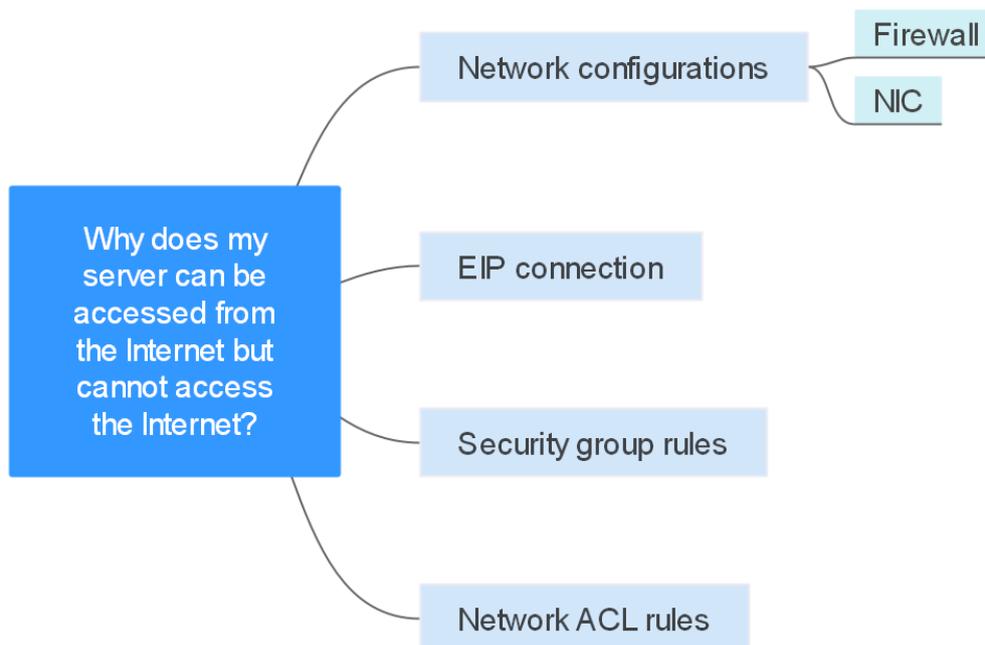


Tabla 8-4 Causas posibles

Causa posible	Solución
Configuraciones de red	Consulte Configuraciones de red
Conexión de EIP	Véase ¿Por qué falla el acceso a Internet incluso si mi ECS está vinculado a un EIP?
Reglas de grupos de seguridad	Consulte Reglas de grupos de seguridad
Reglas de ACL de red	Consulte Reglas de ACL de red

Configuraciones de red

- Firewall

Deshabilite las reglas de firewall para el ECS y compruebe si se ha restaurado la conectividad a Internet:

 - ECS de Linux: [Comprobación de la configuración del firewall.](#)
 - ECS de Windows: [Comprobación de la configuración del firewall.](#)
- NIC

Compruebe las configuraciones de NIC y DNS.

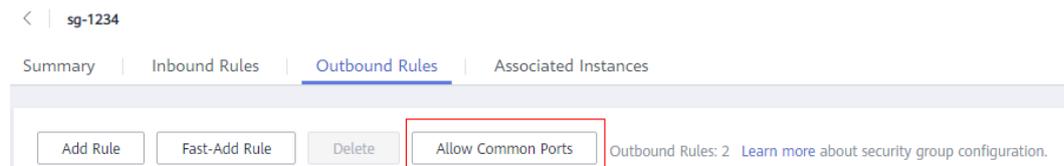
 - ECS de Linux: [Comprobación de la configuración de la NIC.](#)
 - ECS de Windows: [Comprobación de la configuración de la NIC.](#)

Reglas de grupos de seguridad

Compruebe si hay una regla de grupo de seguridad para el servidor que deniega el tráfico saliente.

De forma predeterminada, un grupo de seguridad permite todo el tráfico saliente. Si se deniega el tráfico saliente, puede **configurar reglas de grupo de seguridad** o hacer clic en **Allow Common Ports**.

Figura 8-31 Permitir los puertos comunes

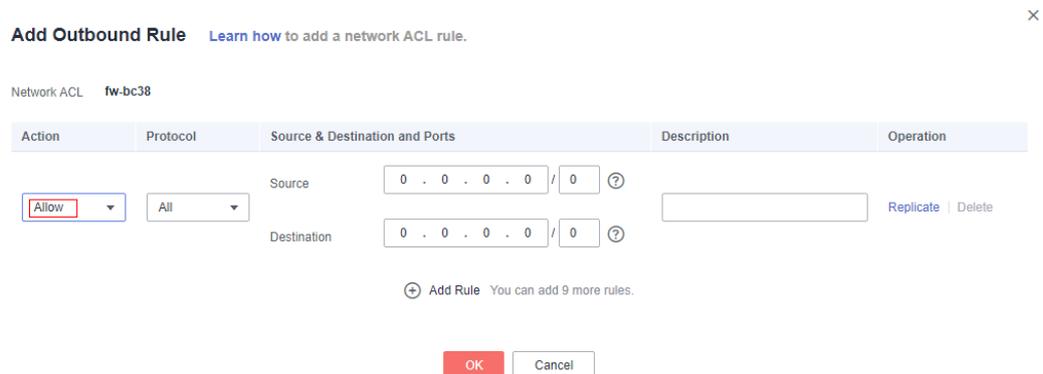


Reglas de ACL de red

Compruebe si la ACL de red de la subred a la que pertenece el servidor niega el tráfico saliente.

De forma predeterminada, una ACL de red niega todo el tráfico saliente. Debe agregar una regla de salida con **Action** establecida en **Permitir** a la ACL de red asociada con el servidor.

Figura 8-32 Permitir el tráfico saliente



Envío de un ticket de servicio

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

8.15 ¿Por qué no puedo acceder a sitios web por las direcciones IPv6 después de configurar la pila dual IPv4/IPv6?

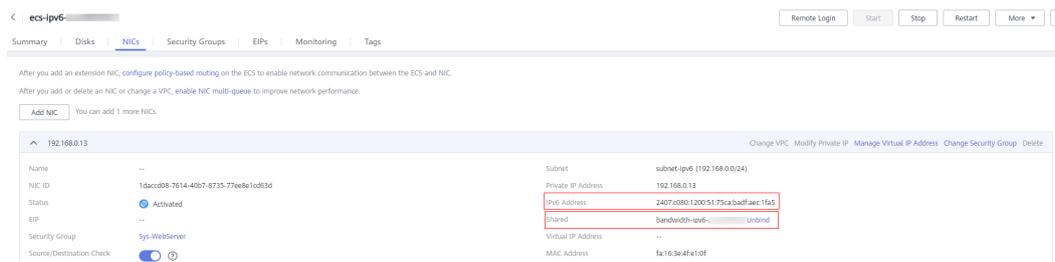
Síntomas

Ha habilitado la doble pila IPv4/IPv6 para un ECS, pero el ECS no puede acceder a sitios web por las direcciones IPv6.

Resolución de problemas

- Compruebe si la doble pila IPv4/IPv6 está correctamente configurada y si la NIC de doble pila del ECS ha obtenido una dirección IPv6.
- Compruebe si la dirección IPv6 obtenida de la NIC de doble pila se ha agregado a un ancho de banda compartido.
- Si el ECS tiene varias NIC, compruebe si se han configurado las rutas basadas en políticas para estas NIC.

Figura 8-33 Detalles de la NIC



Solución

- Cuando compre un ECS, seleccione **Automatically-assigned IPv6 address** para **Network**.

Si una dirección IPv6 no se puede asignar automáticamente o la imagen seleccionada no admite la asignación automática de direcciones IPv6, obtenga manualmente la dirección IPv6 haciendo referencia a [Asignación dinámica de direcciones IPv6](#).

NOTA

Si se crea un ECS a partir de una imagen pública:

Antes de habilitar la asignación dinámica de las direcciones IPv6 para una imagen pública de Linux, compruebe si se admite IPv6 y, a continuación, compruebe si se ha habilitado la asignación dinámica de las direcciones IPv6. Actualmente, todas las imágenes públicas de Linux soportan IPv6, y la asignación dinámica de las direcciones IPv6 está habilitada para Ubuntu 16 por defecto. No es necesario configurar la asignación dinámica de las direcciones IPv6 para Ubuntu 16 OS. Para otras imágenes públicas de Linux, debe habilitar esta función.

- De forma predeterminada, las direcciones IPv6 solo se pueden utilizar para la comunicación de red privada. Si desea utilizar una dirección IPv6 para acceder a Internet o desea que los clientes IPv6 accedan a ella en Internet, debe agregar la dirección IPv6 a un ancho de banda compartido. Para obtener más información, consulte la sección [Comprar un ancho de banda compartido y agregarle la dirección IPv6](#).

Si ya tiene un ancho de banda compartido, agregue la dirección IPv6.

- Si un ECS tiene varias NIC, la NIC principal puede comunicarse con las redes externas de forma predeterminada, pero las NIC de extensión no pueden. Para permitir que las NIC de extensión se comuniquen con obras externas, es necesario configurar las rutas basadas en políticas para estas NIC.

Si su ECS ejecuta Linux, consulte [Configuración de rutas basadas en políticas para un ECS de Linux con varias NIC \(IPv4/IPv6\)](#).

Si su ECS ejecuta Windows, consulte [Configuración de rutas basadas en políticas para un ECS de Windows con varias NIC \(IPv4/IPv6\)](#).

8.16 ¿Por qué mi ECS no se comunica con los otros después de haber instalado el firewall?

Síntomas

Un ECS tiene una única NIC y no puede comunicarse con los otros después de que el ECS tiene un firewall instalado. Un ejemplo de escenario es el siguiente:

En una VPC, hay tres ECS. Los servicios se implementan en ECS 1 y ECS 2, y un firewall de los terceros está instalado en ECS X. El tráfico de ECS 1 y ECS 2 necesita ser filtrado por el firewall de ECS X.

Localización de fallas

Los problemas aquí se describen en orden de la probabilidad de que ocurran.

Solucione el problema descartando las causas descritas aquí, una por una.

Tabla 8-5 Localización de fallas

Causa posible	Solución
Reglas de grupos de seguridad	Consulte Si las reglas de grupo de seguridad están configuradas
Comprobación de origen/destino	Consulte Si la comprobación de origen/destino está deshabilitada
Rutas personalizadas de VPC	Consulte Si se agregan las rutas personalizadas de VPC

Si las reglas de grupo de seguridad están configuradas

Las subredes en la misma VPC pueden comunicarse entre sí. Si el servicio ECS no puede comunicarse con el ECS que tiene el firewall instalado, compruebe si están en el mismo grupo de seguridad.

Si los ECS están en diferentes grupos de seguridad, debe agregar reglas a los grupos de seguridad para permitir el acceso entre sí.

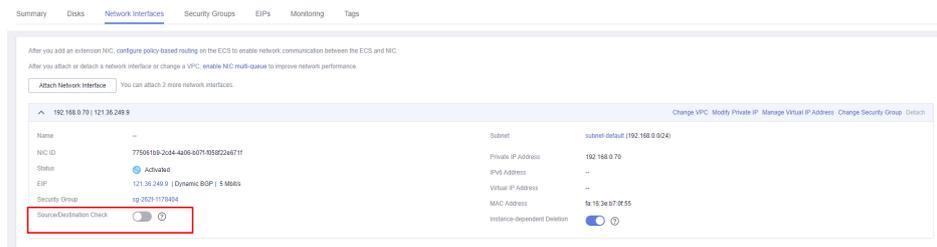
Para obtener más información, consulte [Agregar una regla de grupo de seguridad](#).

Si la comprobación de origen/destino está deshabilitada

Compruebe si la función de comprobación de origen/destino está deshabilitada en la NIC del ECS con firewall instalado. Si la función no está deshabilitada, realice las siguientes operaciones para deshabilitarla:

1. Inicie sesión en la consola de gestión.

- Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
- Haga clic en **Service List** y elija **Compute > Elastic Cloud Server**.
- En la lista de ECS, haga clic en el nombre ECS de destino.
Se muestra la ficha **Summary** del ECS.
- Haga clic en la ficha **NICs** y haga clic en  para ampliar la información sobre la NIC principal y comprobar si **Source/Destination Check** está deshabilitado.
Si no está deshabilitado, desactívelo.



Si se agregan las rutas personalizadas de VPC

Compruebe si la tabla de ruta de la subred del servicio VPC tiene una ruta que apunta al ECS con firewall instalado.

Si no hay tal ruta, agregue una ruta personalizada con el salto siguiente establecido en ECS y el destino establecido en ECS con el firewall instalado.

Para obtener más información, consulte [Agregar una ruta personalizada](#).

Envío de un ticket de servicio

Si el problema persiste, [envíe un ticket de servicio](#).

9 Enrutamiento

9.1 ¿Cómo configuro las rutas basadas en políticas para un ECS con varias NIC?

Guía de operación

Este documento describe cómo configurar las rutas basadas en políticas para los ECS de Linux y Windows. Para obtener más información, véase [Tabla 9-1](#).

Tabla 9-1 Instrucciones de operación

Tipo de SO	Versión de dirección IP	Procedimiento
Linux	IPv4	Tome un ECS que ejecuta CentOS 8.0 (64 bits) como ejemplo. Configuración de rutas basadas en políticas para un ECS de Linux con varias NIC (IPv4/IPv6)
	IPv6	
Windows	IPv4	Tome un ECS que ejecuta Windows Server 2012 (64 bits) como ejemplo. Configuración de rutas basadas en políticas para un ECS de Windows con varias NIC (IPv4/IPv6)
	IPv6	

Operaciones relacionadas

Si desea acceder a Internet mediante una NIC de extensión, consulte [¿Cómo accedo a Internet mediante una vinculación de EIP a una NIC de extensión?](#)

9.2 ¿Una tabla de ruta puede abarcar varias VPC?

Una tabla de ruta no puede abarcar varias VPC.

Una tabla de rutas contiene un conjunto de las rutas que se utilizan para determinar a dónde se dirige el tráfico de red de las subredes en una VPC. Una VPC tiene una tabla de ruta predeterminada y puede tener varias tablas de ruta personalizadas.

Cada subred de una VPC debe estar asociada a una tabla de rutas. Una subred sólo se puede asociar a una tabla de ruta a la vez, pero puede asociar varias subredes en una VPC a la misma tabla de ruta.

9.3 ¿Cuántas rutas puede contener una tabla de rutas?

Cada tabla de rutas puede contener un máximo de rutas de 200 de forma predeterminada, incluidas las rutas agregadas para interconexión de conexión directa y VPC.

9.4 ¿Existen restricciones en el uso de una tabla de rutas?

- Un ECS que proporciona SNAT debe tener activada la opción **Unbind IP from MAC**.
- El destino de cada ruta en una tabla de rutas debe ser único. El salto siguiente debe ser una dirección IP privada o una dirección IP virtual en la VPC. De lo contrario, la tabla de rutas no tendrá efecto.
- Si se establece una dirección IP virtual para que sea el salto siguiente en una ruta, las EIP vinculadas con la dirección IP virtual en la VPC no serán válidas.

9.5 ¿Se facturará una tabla de ruta?

La función de tabla de rutas en sí es gratuita, pero se le cobrará por los ECS y el ancho de banda que utilice junto con la función de tabla de rutas.

9.6 ¿Se aplican las mismas prioridades de enrutamiento a las conexiones de conexión directa y a las rutas personalizadas en la misma VPC?

No. Direct Connect connections and custom routes are used in different scenarios, so the routing priorities are different.

9.7 ¿Hay diferentes prioridades de enrutamiento de la VPN y las rutas personalizadas en la misma VPC?

No. La prioridad de enrutamiento de las rutas personalizadas y la de las VPN son las mismas.

10 Seguridad

10.1 ¿Las reglas del grupo de seguridad se consideran iguales si todos los parámetros, excepto su descripción, son iguales?

Sí. No puede agregar ni importar una regla de grupo de seguridad que tenga los mismos parámetros pero una descripción diferente a una regla existente en el grupo de seguridad.

10.2 ¿Cuáles son los requisitos para eliminar un grupo de seguridad?

- Antes de eliminar un grupo de seguridad, asegúrese de que el grupo de seguridad no esté en uso por los recursos de la nube, como servidores en la nube, contenedores y bases de datos. Si un recurso en la nube utiliza el grupo de seguridad, libere el recurso en la nube o cambie el grupo de seguridad utilizado por el recurso en la nube y, a continuación, elimine el grupo de seguridad.
- Si el grupo de seguridad que desea eliminar está asociado a reglas de otro grupo de seguridad (**Source**), elimine o modifique las reglas de grupo de seguridad asociadas y, a continuación, elimine el grupo de seguridad.

NOTA

- No se puede eliminar el grupo de seguridad predeterminado.
- Si un grupo de seguridad está asociado con recursos que no sean servidores y NIC de extensión, no se puede eliminar el grupo de seguridad.

10.3 ¿Por qué se bloquea el acceso saliente en el puerto TCP 25?

Síntoma

No puede acceder a una dirección externa en el puerto TCP 25. Por ejemplo, la ejecución del comando **Telnet smtp.***.com 25** falla.

Motivo

Por razones de seguridad, el puerto TCP 25 está deshabilitado en la dirección de salida por defecto.

No es necesario habilitar el puerto TCP 25, a menos que desee implementar un servicio de correo electrónico en la nube.

Esta sección solo se aplica a CN-Hong Kong.

Solución

- Utilice el puerto 465 compatible con el proveedor de servicios de correo electrónico de terceros.
- Aplique para habilitar el puerto TCP 25 en la dirección de salida.
Si debe habilitar el puerto TCP 25 en el ECS para comunicaciones externas, envíe una solicitud.

AVISO

Antes de enviar su solicitud, debe aceptar y garantizar que el puerto TCP 25 solo se utiliza para conectarse a servidores de protocolo simple de transferencia de correo (SMTP) de terceros y que los correos electrónicos se envían mediante servidores SMTP de terceros. Si utiliza la EIP especificada en el ticket de servicio para enviar directamente los correos electrónicos a través de SMTP, desactivaremos permanentemente el puerto TCP 25 y ya no podrá usarlo ni solicitar que se active.

-
1. En la página **Create Service Ticket**, elija **Products > Elastic Cloud Server**.
 2. Haga clic en **Open Port 25** en **Select Subtype** y cree un ticket de servicio.
Para obtener más información sobre cómo enviar un ticket de servicio, consulte [Enviar un ticket de servicio](#).

10.4 ¿Cómo distingo las instancias asociadas a un grupo de seguridad?

Un grupo de seguridad se puede asociar con las instancias cuando se crean o después. Para eliminar un grupo de seguridad de este tipo, primero debe desasociar las instancias del grupo de seguridad.

Puede iniciar sesión en la consola de gestión para comprobar las instancias asociadas que se muestran en [Tabla 10-1](#), excepto los servidores, las NIC de extensión y las interfaces de red suplementarias.

Si no puede eliminar un grupo de seguridad incluso después de eliminar todas las instancias asociadas, [envíe un ticket de servicio](#).

Tabla 10-1 Lista de verificación

Categoría del producto	Producto
Base de datos	GaussDB
	RDS
	DDS
	GaussDB NoSQL
	DDM
Middleware	Redis/Memcached
	Kafka
	RabbitMQ
	DMS (for RocketMQ)
	API Gateway
Big data	DGC
	DWS
	CSS

10.5 ¿Puedo cambiar el grupo de seguridad de un ECS?

Sí. Inicie sesión en la consola de ECS, cambie a la página que muestra los detalles de ECS y cambie el grupo de seguridad del ECS.

Para obtener más información, consulte [Cambio de un grupo de seguridad](#).

10.6 ¿Cuántos grupos de seguridad puedo crear?

Cada cuenta puede tener hasta 100 grupos de seguridad y 5000 reglas de grupo de seguridad.

Cuando crea un ECS, puede seleccionar varios grupos de seguridad, pero se recomienda que seleccione no más de cinco.

10.7 ¿Se facturará a un grupo de seguridad?

Los grupos de seguridad son gratuitos.

10.8 ¿Cómo configuro un grupo de seguridad para protocolos multicanal?

Configuración de ECS

El TFTP daemon determina si un archivo de configuración especifica el rango de puertos. Si utiliza un archivo de configuración de TFTP que permite que los puertos del canal de datos sean configurables, es una buena práctica configurar un pequeño rango de puertos que no se escuchan.

Configuración del grupo de seguridad

Puede configurar el puerto 69 y configurar los puertos de canal de datos utilizados por TFTP para el grupo de seguridad. En RFC1350, el protocolo TFTP especifica que los puertos disponibles para los canales de datos van de 0 a 65535. Sin embargo, no todos estos puertos son utilizados por los procesos de TFTP daemon de diferentes aplicaciones. Puede configurar un rango más pequeño de puertos para el TFTP daemon.

La siguiente figura proporciona un ejemplo de la configuración de reglas de grupo de seguridad si los puertos utilizados por los canales de datos varían de 60001 a 60100.

Figura 10-1 Reglas de grupos de seguridad

Type	Protocol	Port/Range	Source
<input type="checkbox"/> IPv4	All	All	sg-test
<input type="checkbox"/> IPv4	UDP	60001-60100	0.0.0.0

10.9 ¿Cuántas ACL de red puedo crear?

Puede crear hasta 200 ACL de red. Se recomienda que no configure más de 20 reglas entrantes o salientes para cada una ACL de red. Si configura más de 20 reglas entrantes o salientes para una ACL de red, el rendimiento del reenvío se deteriorará.

10.10 Does a Security Group Rule or a ACL de red Rule Immediately Take Effect for Existing Connections After It Is Modified?

- After a security group rule is modified, the new rule immediately takes effect for its original traffic. Security groups are stateful. Responses to outbound traffic are allowed to go in to the instance regardless of inbound security group rules, and vice versa. Security groups use connection tracking to track traffic to and from instances. If a security group rule is added, deleted, or modified, or an instance in the security group is created or deleted, the connection tracking for all instances in the security group will be automatically cleared. In this case, the inbound or outbound traffic of the instance will be considered to be new connections, which need to match the inbound or outbound security group rules to ensure that the rules take effect immediately and ensure the security of incoming traffic.

- A modified ACL de red rule will not immediately take effect for its existing connections. It takes about 120 seconds for the new rule to take effect, and traffic will be interrupted during this period. To ensure that the traffic is immediately interrupted after the rule is changed, it is recommended that you configure security group rules.

10.11 ¿Por qué algunos puertos son inaccesibles?

Symptom: Los usuarios en ciertas áreas no pueden acceder a algunos puertos.

Analysis: Los puertos enumerados en la siguiente tabla son puertos de alto riesgo y están bloqueados de forma predeterminada.

Tabla 10-2 Puertos de alto riesgo

Protocolo	Puerto
TCP	42, 135, 137, 138, 139, 444, 445, 593, 1025, 1068, 1433, 1434, 3127, 3128, 3129, 3130, 4444, 4789, 5554, 5800, 5900, 8998, 9995, y 9996
UDP	135 a 139, 1026, 1027, 1028, 1068, 1433, 1434, 4789, 5554, 9995, y 9996

Solución: se recomienda utilizar los puertos que no aparecen en la tabla para los servicios.

10.12 ¿Por qué todavía se permite el acceso desde una dirección IP específica después de que se haya agregado una regla de ACL de red que niega el acceso desde la dirección IP?

Las reglas de ACL de red tienen prioridades. Un valor de prioridad más pequeño indica una prioridad más alta. Cada ACL de red incluye una regla predeterminada cuyo valor de prioridad es un asterisco (*). Las reglas predeterminadas tienen la prioridad más baja.

Si las reglas entran en conflicto, la regla con la prioridad más alta entra en vigor.

Si necesita que una regla surta efecto antes o después de una regla específica, puede insertar esa regla antes o después de la regla específica. Por ejemplo, si la prioridad de la regla A es 1 pero necesita que la regla B tenga prioridad sobre la regla A, inserte la regla B antes que la regla A. Entonces, la regla B tendrá una prioridad de 1 y la regla A será 2. Del mismo modo, si la regla B es menos importante que la regla A, inserte la regla B después de la regla A.

Cuando se agrega una regla que deniega el acceso desde una dirección IP especificada, inserte las reglas que permiten el acceso desde todas las direcciones IP al final. Entonces, la regla que deniega el acceso desde la dirección IP especificada tendrá prioridad sobre las otras reglas y será efectiva. Para obtener más información, consulte la sección [Cambio de la secuencia de una regla de ACL de red](#).

10.13 ¿Por qué no entran en vigor las reglas de mi grupo de seguridad?

Síntomas

Las reglas de grupo de seguridad que ha configurado para un ECS no han surtido efecto.

Resolución de problemas

Los problemas aquí se describen en orden de la probabilidad de que ocurran.

Solucione el problema descartando las causas descritas aquí, una por una.

Figura 10-2 Resolución de problemas

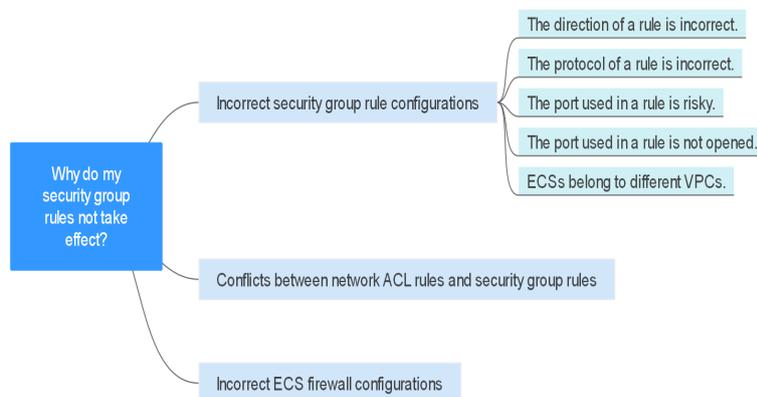


Tabla 10-3 Resolución de problemas

Causa posible	Solución
Configuraciones de regla de grupo de seguridad incorrectas	Consulte Configuración de regla de grupo de seguridad incorrecta
Conflictos entre las reglas de ACL de red y las reglas de grupo de seguridad	Consulte Conflictos entre las reglas de ACL de red y las reglas de grupo de seguridad
Configuraciones de firewall de ECS incorrectas	Consulte Configuraciones de firewall de ECS incorrectas

Configuración de regla de grupo de seguridad incorrecta

Si las reglas de grupo de seguridad no se configuran correctamente, los ECS no se pueden proteger. Compruebe las reglas del grupo de seguridad basadas en las siguientes causas:

1. La dirección de una regla es incorrecta.
2. El protocolo de una regla es incorrecto.
3. El puerto utilizado en una regla es arriesgado y no se puede acceder a él. Para obtener más información acerca de los puertos comunes y los puertos riesgosos, consulte [Puertos comunes utilizados por ECS](#).
4. El puerto utilizado en una regla no se abre. Puede realizar los siguientes pasos para comprobar si se está escuchando un puerto en el servidor.

Por ejemplo, ha implementado un sitio web en ECS. Los usuarios deben acceder a su sitio web a través de TCP (puerto 80), y usted ha agregado la regla de grupo de seguridad que se muestra en [Tabla 10-4](#).

Tabla 10-4 Regla del grupo de seguridad

Dirección	Protocolo	Puerto	Fuente
Entrante	TCP	80	0.0.0.0/0

ECS de Linux

Para verificar la regla de grupo de seguridad en un ECS de Linux:

- a. Inicie sesión en el ECS.
- b. Ejecute el siguiente comando para comprobar si se está escuchando el puerto TCP 80:

```
netstat -an | grep 80
```

Si se muestra la salida del comando en [Figura 10-3](#), se está escuchando el puerto TCP 80.

Figura 10-3 Salida del comando para ECS de Linux

```
tcp      0      0 0.0.0.0:80          0.0.0.0:*        LISTEN
```

- c. Escriba `http://ECS EIP` en el cuadro de dirección del navegador y pulse **Enter**. Si se puede acceder a la página solicitada, la regla del grupo de seguridad tiene efecto.

ECS de Windows

Para comprobar la regla del grupo de seguridad en un ECS de Windows:

- a. Inicie sesión en el ECS.
- b. Elija **Start > Accessories > Command Prompt**.
- c. Ejecute el siguiente comando para comprobar si se está escuchando el puerto TCP 80:

```
netstat -an | findstr 80
```

Si se muestra la salida del comando en [Figura 10-4](#), se está escuchando el puerto TCP 80.

Figura 10-4 Salida del comando para Windows ECS

```
TCP      0.0.0.0:80          0.0.0.0:0        LISTENING
```

- d. Escriba **http://ECS EIP** en el cuadro de dirección del navegador y pulse **Enter**. Si se puede acceder a la página solicitada, la regla del grupo de seguridad tiene efecto.
5. Los ECS pertenecen a las diferentes VPC. Si dos ECS están en el mismo grupo de seguridad pero en las VPC diferentes, los ECS no pueden comunicarse entre sí. Para habilitar las comunicaciones entre los ECS, utilice una interconexión de VPC para conectar los dos VPC. Para obtener detalles sobre la conectividad de VPC, consulte [Escenarios de aplicación](#).

Puede [agregar una regla de grupo de seguridad](#) o [modificar una regla de grupo de seguridad](#) para seleccionar la dirección correcta, el protocolo y abrir los puertos.

Conflictos entre las reglas de ACL de red y las reglas de grupo de seguridad

Los grupos de seguridad operan a nivel de ECS, mientras que las ACL de red operan a nivel de subred.

Por ejemplo, si configura una regla de grupo de seguridad entrante para permitir el acceso a través del puerto 80 y una regla de ACL de red para denegar el acceso a través del puerto 80, la regla de grupo de seguridad no tendrá efecto.

Puede [agregar una regla de ACL de red](#) o [modificar una regla de ACL de red](#) para permitir el tráfico desde el puerto de protocolo correspondiente.

Configuraciones de firewall de ECS incorrectas

Compruebe si el firewall del ECS abre los puertos requeridos.

Para obtener más información, consulte [Desactivar un Firewall de ECS de Windows y agregar una excepción de puerto en un Firewall de ECS de Windows](#) o [Desactivar un Firewall de ECS de Linux y agregar una excepción de puerto en un Firewall de ECS de Linux](#).

Envío de un ticket de servicio

Si el problema persiste, [envíe un ticket de servicio](#).