nube privada virtual

Guía del usuario

Edición 01

Fecha 2024-09-18

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


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 VPC y subred

1.1 Planificación de redes

Antes de crear sus VPC, determine cuántas VPC, el número de las subredes y qué rangos de direcciones IP o opciones de conectividad necesitará.

¿Cómo puedo determinar cuántas VPC necesito?

Las VPC son específicas de la región. De forma predeterminada, las redes de VPC en diferentes regiones o incluso en la misma región no están conectadas. Las redes en diferentes VPC están completamente aisladas entre sí, este no es el caso de redes en la misma VPC sino en diferentes AZ. Las redes en la misma VPC pueden comunicarse entre sí incluso si están en diferentes AZ.

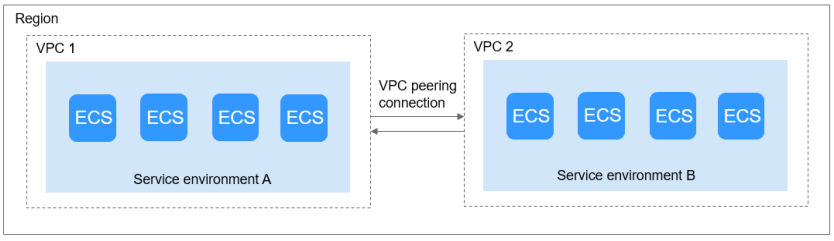
Una VPC

Si sus servicios no requieren aislamiento de red, una sola VPC debería ser suficiente.

Múltiples VPC

Si tiene varios sistemas de servicio en una región y cada sistema de servicio requiere una red aislada, puede crear una VPC independiente para cada sistema de servicio. Si necesita conectividad de red entre las VPC independientes, puede utilizar una interconexión de VPC como se muestra en **Figura 1-1**.

Figura 1-1 Interconexión de VPC



¿Cómo planeo las subredes?

Una subred es un bloque CIDR único con un rango de las direcciones IP en una VPC. Todos los recursos de una VPC deben implementarse en las subredes.

- De forma predeterminada, los ECS de todas las subredes de la misma VPC pueden comunicarse entre sí, pero los ECS de las diferentes VPC no pueden.

  Puede crear interconexión de VPC para habilitar ECS en diferentes VPC pero en la misma región para comunicarse entre sí.
- Después de que se crea una subred, su CIDR no se puede modificar.

  Las subredes utilizadas para implementar sus recursos deben residir dentro de su VPC, y las máscaras de subred utilizadas para definirlas pueden estar entre la máscara de red de su bloque CIDR de VPC y /28 Máscara de red.
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

  NOTA

  Una máscara de subred puede estar entre la máscara de red de su bloque CIDR de VPC y la máscara de red /28. Si un bloque CIDR de VPC es 192.168.0.0/16, su máscara de subred puede estar entre 16 y 28.

Planificación de subred

- Recomendamos crear diferentes subredes para diferentes módulos de servicio en una VPC. Por ejemplo, puede crear diferentes subredes para los servidores web, de aplicaciones y de bases de datos. Un servidor web está en una subred de acceso público, y los servidores de aplicaciones y de bases de datos están en las subredes de acceso no público. Puede aprovechar las ACL de red para ayudar a controlar el acceso a los servidores de cada subred.
- Si solo necesita planificar subredes para VPC, y la comunicación entre VPC y centros de datos locales no es necesaria, puede crear subredes dentro de cualquiera de los bloques CIDR enumerados anteriormente.
- Si su VPC necesita comunicarse con un centro de datos local a través de VPN o Direct Connect, el bloque CIDR de VPC no puede solaparse con el bloque CIDR del centro de datos local. Por lo tanto, al crear una VPC o subred, asegúrese de que su bloque CIDR no se superponga con ningún bloque CIDR en el centro de datos.
- Al determinar el tamaño de un bloque CIDR de VPC o subred, asegúrese de que el número de direcciones IP disponibles en el bloque CIDR cumpla con sus requisitos de servicio.

Cuota de subred predeterminada

De forma predeterminada, puede crear hasta 100 subredes en su cuenta. Si necesita más, solicite un aumento de cuota.

¿Cómo planeo las políticas de enrutamiento?

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. Cuando crea una VPC, tiene automáticamente una tabla de rutas predeterminada, que permite la comunicación interna dentro de esa VPC.

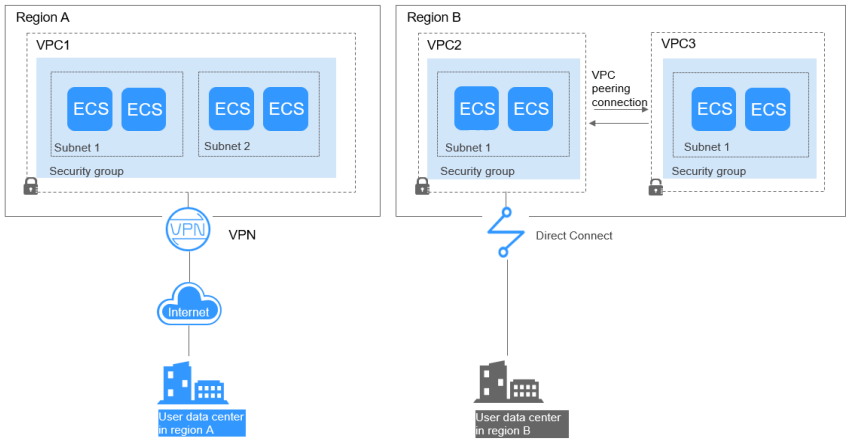
- Si no necesita controlar explícitamente cómo cada subred enruta el tráfico entrante y saliente, puede utilizar la tabla de rutas predeterminada.
- Si necesita controlar explícitamente cómo cada subred enruta el tráfico entrante y saliente en una VPC, puede agregar rutas personalizadas a la tabla de rutas.

¿Cómo me conecto a un centro de datos local?

Si necesita la interconexión entre una VPC y un centro de datos local, asegúrese de que la VPC no tenga un rango de direcciones IP superpuesto con el centro de datos local que se va a conectar.

Como se muestra en **Figura 1-2**, usted tiene VPC 1 en la región A y VPC 2 y VPC 3 en la región B. Para conectarse a un centro de datos local, pueden usar una VPN, como lo hace la VPC 1 en la región A; o una conexión de Direct Connect, como lo hace la VPC 2 en la región B. La VPC 2 se conecta al centro de datos a través de una conexión de Direct Connect, pero para conectarse a otra VPC en esa región, como la VPC 3, se debe establecer un interconexión de VPC.

Figura 1-2 Conexiones a centros de datos locales



Al planificar los bloques CIDR para VPC 1, VPC 2 y VPC 3.

- El bloque CIDR de la VPC 1 no puede solaparse con el bloque CIDR del centro de datos local en la región A.
- El bloque CIDR de la VPC 2 no puede solaparse con el bloque CIDR del centro de datos local en la Región B.
- Los bloques CIDR de la VPC 2 y la VPC 3 no pueden solaparse.

¿Cómo accedo a Internet?

Utilice los EIP para permitir que un pequeño número de ECS accedan a Internet.

Cuando solo unos pocos ECS necesitan acceder a Internet, puede vincular las EIP a los ECS. Esto les proporcionará acceso a Internet. También puede desvincular dinámicamente las EIP de los ECS y vincularlos a los gateway de NAT y los balanceadores de carga en su lugar, que también proporcionará acceso a Internet. El proceso no es complicado.

Utilice un gateway de NAT para permitir que un gran número de ECS accedan a Internet.

Cuando un gran número de ECS necesitan acceder a Internet, la nube pública proporciona los gateway de NAT para sus ECS. Con los gateway de NAT, no es necesario asignar una EIP a cada ECS. Los gateway de NAT reducen los costos ya que no necesita tantas EIP. Los gateway de NAT ofrecen tanto la traducción de direcciones de red de origen (SNAT) como la traducción de direcciones de red de destino (DNAT). SNAT permite que varios ECS en la misma VPC compartan uno o más EIP para acceder a Internet. SNAT evita que las EIP de ECS sean expuestas a Internet. DNAT puede implementar el reenvío de datos por puerto. Asigna puertos de EIP a puertos de ECS para que los ECS de una VPC puedan compartir la misma EIP y el mismo ancho de banda para proporcionar servicios accesibles a Internet.

Utilice ELB para acceder a Internet si hay un gran número de solicitudes simultáneas.

En escenarios de alta simultaneidad, como el comercio electrónico, puede utilizar los balanceadores de carga proporcionados por el servicio de ELB para distribuir uniformemente el tráfico entrante entre múltiples ECS, lo que permite que un gran número de usuarios accedan simultáneamente a su sistema o a la aplicación empresarial. ELB se implementa en el modo de clúster. Proporciona tolerancia a fallos para sus aplicaciones al equilibrar automáticamente el tráfico a través de múltiples AZ. También puede aprovechar la integración profunda con Auto Scaling (AS), que permite el ajuste automático basado en el tráfico de servicio y garantiza la estabilidad y fiabilidad del servicio.

1.2 VPC

1.2.1 Creación de una VPC

Escenarios

Las VPC proporcionan una red virtual aislada para los ECS. Puede configurar y gestionar la red según sea necesario.

Puede crear una VPC siguiendo el procedimiento proporcionado en esta sección. A continuación, cree subredes, grupos de seguridad y asigne las EIP siguiendo el procedimiento proporcionado en las secciones posteriores según los requisitos reales de la red.

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. Haga clic en **Create VPC**.

   Se muestra la página **Create VPC**.
4. En la página **Create VPC**, establezca los parámetros según se le solicite.

   Se creará una subred predeterminada junto con una VPC y también puede hacer clic en **Add Subnet** para crear más subredes para la VPC.

Figura 1-3 Creación de una VPC y una subred

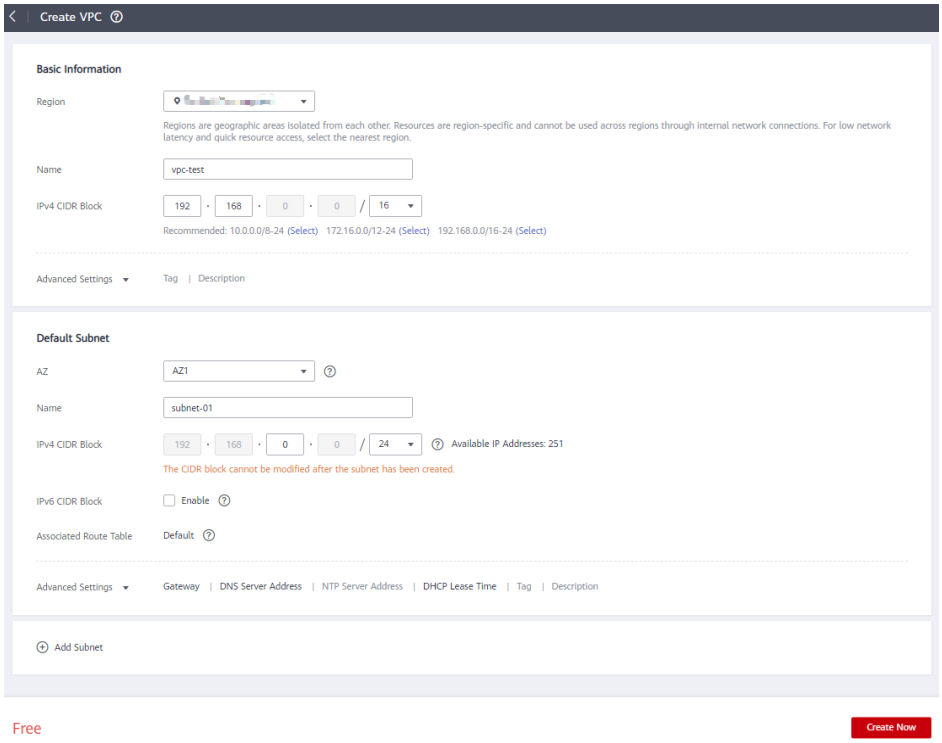


Tabla 1-1 Descripciones de parámetro de VPC

Parámetro	Descripción	Valor de ejemplo
Region	Las regiones son áreas geográficas que están físicamente aisladas unas de otras. Las redes dentro de diferentes regiones no están conectadas entre sí, por lo que los recursos no se pueden compartir entre diferentes regiones. Para una menor latencia de red y un acceso más rápido a sus recursos, seleccione la región más cercana a usted.	CN-Hong Kong
Name	El nombre de la VPC. El nombre puede contener un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios.	VPC-test

Parámetro	Descripción	Valor de ejemplo
CIDR Block or IPv4 CIDR Block	El bloque CIDR de la VPC. El bloque CIDR de una subred puede ser el mismo que el bloque CIDR para la VPC (para una sola subred en la VPC) o un subconjunto del bloque CIDR para la VPC (para múltiples subredes en la VPC). Se admiten los siguientes bloques CIDR: ● 10.0.0.0/8-24 ● 172.16.0.0/12-24 ● 192.168.0.0/16-24 Este parámetro será **CIDR Block** en regiones donde no se admite la pila dual IPv4/IPv6, y **IPv4 CIDR Block** si se admite la pila dual IPv4/IPv6.	192.168.0.0/16
Enterprise Project	El proyecto de empresa al que pertenece la VPC. Un proyecto empresarial facilita la gestión a nivel de proyectos y el agrupamiento de los recursos y usuarios en la nube. El nombre del proyecto predeterminado es **default**. Para obtener más información sobre la creación y gestión de proyectos de empresa.	default
Tag	La etiqueta VPC, que consiste en un par clave y valor. Puede agregar un máximo de 10 etiquetas a cada VPC.	● Clave: vpc_key1 ● Valor: vpc-01
Description	Información complementaria sobre la VPC. Este parámetro es opcional. La descripción de la VPC puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

Tabla 1-2 Descripciones de parámetros de subred

Parámetro	Descripción	Valor de ejemplo
AZ	Una AZ es una ubicación geográfica con fuente de alimentación independiente y instalaciones de red en una región. Las AZ están físicamente aisladas, y las AZ de la misma VPC están interconectadas a través de una red interna. Tenga en cuenta lo siguiente cuando seleccione una AZ: ● Una VPC puede tener las subredes que están en las diferentes AZ. Por ejemplo, una VPC puede tener una subred A en AZ 1, y una subred B en AZ 3. ● Un recurso en la nube y su subred pueden estar en las diferentes AZ. Por ejemplo, un servidor en la nube en AZ 1 puede usar una subred en AZ 3.	AZ1
Name	El nombre de la subred. El nombre puede contener un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios.	subnet-01
CIDR Block	El bloque CIDR para la subred. Este valor debe estar dentro del bloque CIDR de VPC. Este parámetro sólo se muestra en regiones donde no se admite la pila dual IPv4/IPv6.	192.168.0.0/24
IPv4 CIDR Block	El bloque CIDR para la subred. Este valor debe estar dentro del bloque CIDR de VPC. Este parámetro sólo se muestra en regiones donde se admite la doble pila IPv4/IPv6.	192.168.0.0/24

Parámetro	Descripción	Valor de ejemplo
IPv6 CIDR Block	Especifica si se debe establecer **IPv6 CIDR Block** en **Enable**. Una vez activada la función IPv6, el sistema asigna automáticamente un bloque CIDR IPv6 a la subred creada. Actualmente, el bloque CIDR IPv6 no se puede personalizar. La IPv6 no se puede deshabilitar después de haber creado la subred. Este parámetro sólo se muestra en regiones donde se admite la doble pila IPv4/IPv6.	-
Associated Route Table	Tabla de rutas predeterminada a la que se asociará la subred. Puede cambiar la tabla de rutas a una tabla de rutas personalizada en la página **Subnets**.	Default
Advanced Settings	Haga clic en la flecha desplegable para establecer la configuración avanzada de la subred, incluidas **Gateway** y **DNS Server Address**.	Default
Gateway	La dirección del gateway de la subred. Esta dirección IP se utiliza para comunicarse con otras subredes.	192.168.0.1

Parámetro	Descripción	Valor de ejemplo
NTP Server Address	La dirección IP del servidor de NTP. Este parámetro es opcional. Puede configurar las direcciones IP del servidor de NTP para agregarse a la subred según sea necesario. Las direcciones IP se agregan además de las direcciones de servidor de NTP predeterminadas. Si este parámetro se deja vacío, no se agrega ninguna dirección IP del servidor NTP. Ingrese cuatro direcciones IP válidas como máximo y sepárelas con comas. Cada dirección IP debe ser única. Si agrega o cambia las direcciones del servidor de NTP de una subred, debe renovar la concesión DHCP o reiniciar todos los ECS de la subred para que el cambio surta efecto inmediatamente. Si las direcciones del servidor de NTP se han borrado, reiniciar los ECS no ayudará. Debe renovar la concesión DHCP para de todos los ECS para que el cambio se aplique inmediatamente.	192.168.2.1
DNS Server Address	Las direcciones de servidor de DNS permiten que los ECS de una subred de VPC se comuniquen entre sí mediante nombres de dominio privados. También puede acceder directamente a los servicios en la nube a través de servidores DNS privados. Si desea utilizar otros servidores de DNS públicos para la resolución, puede cambiar las direcciones del servidor DNS predeterminado. También puede hacer clic en **Reset** a la derecha para restaurar las direcciones del servidor DNS al valor predeterminado. Se puede configurar un máximo de dos direcciones IP del servidor de DNS. Varias direcciones IP deben separarse mediante las comas (,).	100.125.x.x

Parámetro	Descripción	Valor de ejemplo
DHCP Lease Time	Período durante el cual un cliente puede utilizar una dirección IP asignada automáticamente por el servidor de DHCP. Una vez expirado el período de concesión, se asignará una nueva dirección IP al cliente. ● Limitado: Establezca el tiempo de concesión DHCP. La unidad puede ser de día u hora. ● Ilimitado: el tiempo de concesión DHCP no expira. Si se cambia el tiempo de la concesión DHCP, la nueva concesión se aplica automáticamente cuando ha pasado la mitad del tiempo de la concesión actual. Para aplicar el cambio inmediatamente, reinicie el ECS o acceda al ECS para generar la renovación automática de la concesión DHCP.	365 days
Tag	La etiqueta de subred, que consiste en un par clave y valor. Puede agregar un máximo de 10 etiquetas a cada subred.	● Key: subnet_key1 ● Value: subnet-01
Description	Información complementaria sobre la subred. Este parámetro es opcional. La descripción de la subred puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

Tabla 1-3 Clave de etiqueta de VPC y requisitos de valor

Parámetro	Requerimientos	Valor de ejemplo
Key	● No se puede dejar en blanco. ● Debe ser único para la misma VPC y puede ser el mismo para las diferentes VPC. ● Puede contener un máximo de 36 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), y guiones (-).	vpc_key1

Parámetro	Requerimientos	Valor de ejemplo
Value	● Puede contener un máximo de 43 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), puntos (.) y guiones (-).	vpc-01

Tabla 1-4 Clave de etiqueta de subred y requisitos de valor

Parámetro	Requerimientos	Valor de ejemplo
Key	● No se puede dejar en blanco. ● Debe ser único para cada subred. ● Puede contener un máximo de 36 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), y guiones (-).	subnet_key1
Value	● Puede contener un máximo de 43 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), puntos (.) y guiones (-).	subnet-01

5. Confirme la configuración actual y haga clic en **Create Now**.

1.2.2 Modificación de una VPC

Escenarios

Cambie el nombre de la VPC y el bloque CIDR.

Si el bloque CIDR de VPC entra en conflicto con el bloque CIDR de una VPN creada en la VPC, puede modificar su bloque CIDR.

Notas y restricciones

- Si se admite la adición de un bloque CIDR IPv4 secundario a una VPC, no se puede modificar el bloque CIDR de una VPC existente en la consola. Sin embargo, puede usar las API para modificar el bloque CIDR de una VPC existente.

  Actualmente, los bloques CIDR IPv4 secundarios para VPC solo están disponibles en **AP-Singapore** y **CN North-Beijing4**.

  NOTA

  Si una VPC tiene una subred en su bloque CIDR secundario, el bloque CIDR secundario no se puede modificar en la consola o usando API.

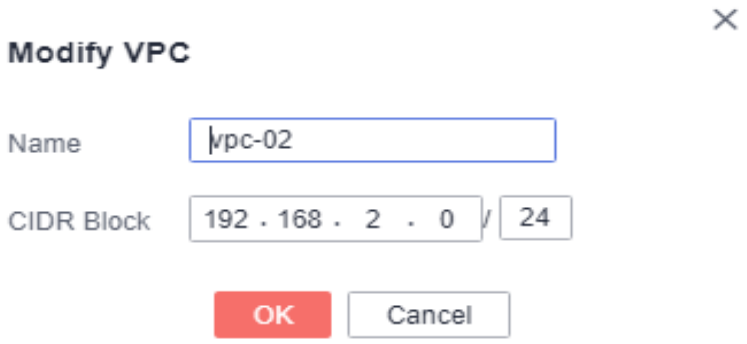
- Al modificar el bloque CIDR de VPC:
  - El bloque CIDR de VPC que se va a modificar debe estar en los bloques CIDR compatibles: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, y 192.168.0.0 – 192.168.255.255

– Si la VPC tiene subredes, el bloque CIDR de la VPC que se va a modificar debe contener todos los bloques CIDR de la subred.

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 panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
4. En la página **Virtual Private Cloud**, busque la fila que contiene la VPC que se va a modificar y haga clic en **Modify** o **Edit CIDR Block** en la columna **Operation**.
5. En la página mostrada, modifique los parámetros según se le solicite. **Figura 1-4** muestra la captura de pantalla.

Figura 1-4 Modificar la VPC



6. Haga clic en **OK**.

1.2.3 Adding a Secondary CIDR Block to a VPC

Scenarios

When you create a VPC, you must specify a CIDR block for the VPC. This is the primary CIDR block of your VPC, and it cannot be modified after the VPC is created.

To extend the IP address range of your VPC, you can add a secondary CIDR block.

If you need to create a subnet in the VPC, you can select either the primary or the secondary CIDR block. Similar to the primary CIDR block, if you create a subnet in the secondary CIDR block, a route is automatically added to your VPC route table to enable routing within the VPC.

NOTA

- Secondary CIDR blocks are now available only in regions CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.
- If adding a secondary IPv4 CIDR block to a VPC is supported, you can only use APIs to modify the CIDR block of an existing VPC. For details, see the **Virtual Private Cloud API Reference**.

Notes and Constraints

- By default, each VPC only can has one secondary IPv4 CIDR block associated.
- If a subnet in a secondary CIDR block of your VPC is the same as or overlaps with the destination of an existing route in the VPC route table, the existing route does not take effect.

  If you create a subnet in a secondary CIDR block of your VPC, a route (the destination is the subnet CIDR block and the next hop is **Local**) is automatically added to your VPC route table. This route allows communications within the VPC and has a higher priority than any other routes in the VPC route table. For example, if a VPC route table has a route with the VPC peering connection as the next hop and 100.20.0.0/24 as the destination, and a route for the subnet in the secondary CIDR block has a destination of 100.20.0.0/16, 100.20.0.0/16 and 100.20.0.0/24 overlaps and traffic will be forwarded through the route of the subnet.
- Tabla 1-5 lists the secondary CIDR blocks that are not supported.

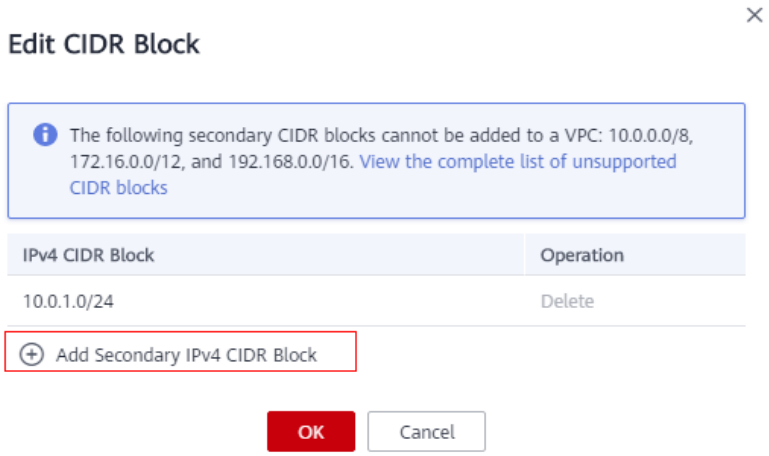
Tabla 1-5 Restricted secondary CIDR blocks

Type	CIDR Block (Not Supported)
Primary CIDR blocks and existing CIDR blocks	● 10.0.0.0/8 ● 172.16.0.0/12 ● 192.168.0.0/16
Reserved system CIDR blocks	● 100.64.0.0/10 ● 214.0.0.0/7 ● 198.18.0.0/15 ● 169.254.0.0/16
Reserved public CIDR blocks	● 0.0.0.0/8 ● 127.0.0.0/8 ● 240.0.0.0/4 ● 255.255.255.255/32

Procedure

1. Log in to the management console.
2. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
3. En la página **Virtual Private Cloud**, busque la fila que contiene la VPC que se va a modificar y haga clic en **Modify** o **Edit CIDR Block** en la columna **Operation**.
4. Click **Add Secondary IPv4 CIDR Block**.

Figura 1-5 Add Secondary IPv4 CIDR Block



5. Enter the secondary CIDR block and click **OK**.

1.2.4 Eliminación de un bloque CIDR secundario de una VPC

Escenarios

Puede eliminar un bloque CIDR secundario de una VPC si ya no lo necesita.

No puede quitar el bloque CIDR IPv4 principal.

NOTA

- Secondary CIDR blocks are now available only in regions CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.
- If adding a secondary IPv4 CIDR block to a VPC is supported, you can only use APIs to modify the CIDR block of an existing VPC. For details, see the **Virtual Private Cloud API Reference**.

Prerrequisitos

Se han eliminado todas las subredes del bloque CIDR secundario.

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 panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
4. En la lista de VPC, busque la fila que contiene la VPC de la que desea eliminar un bloque CIDR secundario y haga clic en **Edit CIDR Block** en la columna **Operation**.
5. Busque la fila que contiene el bloque CIDR secundario que se va a eliminar y haga clic en **Delete** en la columna **Operation**.

1.2.5 Eliminación de una VPC

Escenarios

Puede eliminar una VPC si ya no es necesaria.

Puede eliminar una VPC solo si no hay recursos en esta. Si hay recursos en la VPC, debe eliminar esos recursos antes de poder eliminarla.

No se puede eliminar una VPC si contiene subredes, conexiones de Direct Connect, rutas personalizadas, interconexión de VPC o VPN. Para eliminar la VPC, primero debe eliminar los siguientes recursos.

- Subredes. Para obtener más información, consulte la sección **Supresión de una subred**.
- Conexiones de VPN.
- Conexiones de Direct Connect.
- Rutas personalizadas. Para obtener más información, consulte la sección **Eliminación de una ruta**.
- interconexión de VPC. Para obtener más información, consulte la sección **Eliminación de una interconexión de VPC**.

Notas y restricciones

Si se tienen las EIP o los grupos de seguridad, la última VPC no se puede eliminar.

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 panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
4. En la página **Virtual Private Cloud**, busque la fila que contiene la VPC que se va a eliminar y haga clic en **Delete** en la columna **Operation**.
5. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

1.2.6 Gestión de etiqutas de VPC

Escenarios

Una etiqueta de VPC identifica una VPC. Se pueden agregar etiquetas a las VPC para facilitar sus identificación y gestión. Puede agregar una etiqueta a una VPC al crearla, o puede agregar una etiqueta a una VPC creada en su página de detalles. Se puede añadir un máximo de 10 etiquetas a cada VPC.

Una etiqueta consiste en un par clave y valor. **Tabla 1-6** enumera los requisitos de valor y clave de etiqueta.

Tabla 1-6 Clave de etiqueta de VPC y requisitos de valor

Parámetro	Requerimientos	Valor de ejemplo
Key	● No se puede dejar en blanco. ● Debe ser único para la misma VPC y puede ser el mismo para las diferentes VPC. ● Puede contener un máximo de 36 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), y guiones (-).	vpc_key1
Value	● Puede contener un máximo de 43 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), puntos (.) y guiones (-).	vpc-01

Procedimiento

Busque la VPC por la clave de etiqueta y el valor en la página que muestra la lista de VPC.

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
5. En la esquina superior derecha de la lista de VPC, haga clic en **Search by Tag**.
6. En el área mostrada, introduzca la clave de etiqueta y el valor de la VPC que está buscando.

   Se deben especificar tanto la clave de etiqueta como el valor. El sistema muestra automáticamente las VPC que está buscando si tanto la clave de etiqueta como el valor coinciden.
7. Haga clic en + para agregar más claves de etiqueta y valores.

   Se pueden agregar múltiples claves y valores de etiquetas para restringir los resultados de la búsqueda. Si agrega más de una etiqueta para buscar VPC, se mostrarán las VPC que contienen todas las etiquetas especificadas.
8. Haga clic en **Search**.

   El sistema muestra las VPC que está buscando en función de las claves de etiqueta y los valores introducidos.

Agregar, eliminar, editar y ver etiquetas en la ficha Tags de una VPC.

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.

4. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
5. En la página **Virtual Private Cloud**, localice la VPC cuyas etiquetas se van a gestionar y haga clic en el nombre de la VPC.

   Se muestra la página que muestra detalles sobre la VPC en particular.
6. Haga clic en la ficha **Tags** y realice las operaciones deseadas en las etiquetas.
   - Consulte etiquetas.

     En la ficha **Tags**, puede ver detalles sobre las etiquetas agregadas a la VPC actual, incluido el número de etiquetas y la clave y el valor de cada etiqueta.
   - Agregue una etiqueta.

     Haga clic en **Add Tag** en la esquina superior izquierda. En el cuadro de diálogo **Add Tag** que se muestra, escriba la clave y el valor de la etiqueta y haga clic en **OK**.
   - Edite una etiqueta.

     Busque la fila que contiene la etiqueta que desea editar y haga clic en **Edit** en la columna **Operation**. En el cuadro de diálogo **Edit Tag**, cambie el valor de la etiqueta y haga clic en **OK**.
   - Elimine una etiqueta.

     Busque la fila que contiene la etiqueta que desea eliminar y haga clic en **Delete** en la columna **Operation**. En la caja de diálogo que aparece, haga clic en **Yes**.

1.2.7 Exportación de lista de VPC

Escenarios

La información sobre todas las VPC de su cuenta se puede exportar como un archivo de Excel a un directorio local. Este archivo registra los nombres, ID, estado, intervalos de direcciones IP de las VPC y el número de subredes.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
5. En la esquina superior derecha de la lista de VPC, haga clic en  .

   El sistema exportará automáticamente la información sobre todas las VPC de su cuenta en la región actual. Se exportarán en formato Excel.

1.2.8 Viewing a VPC Topology

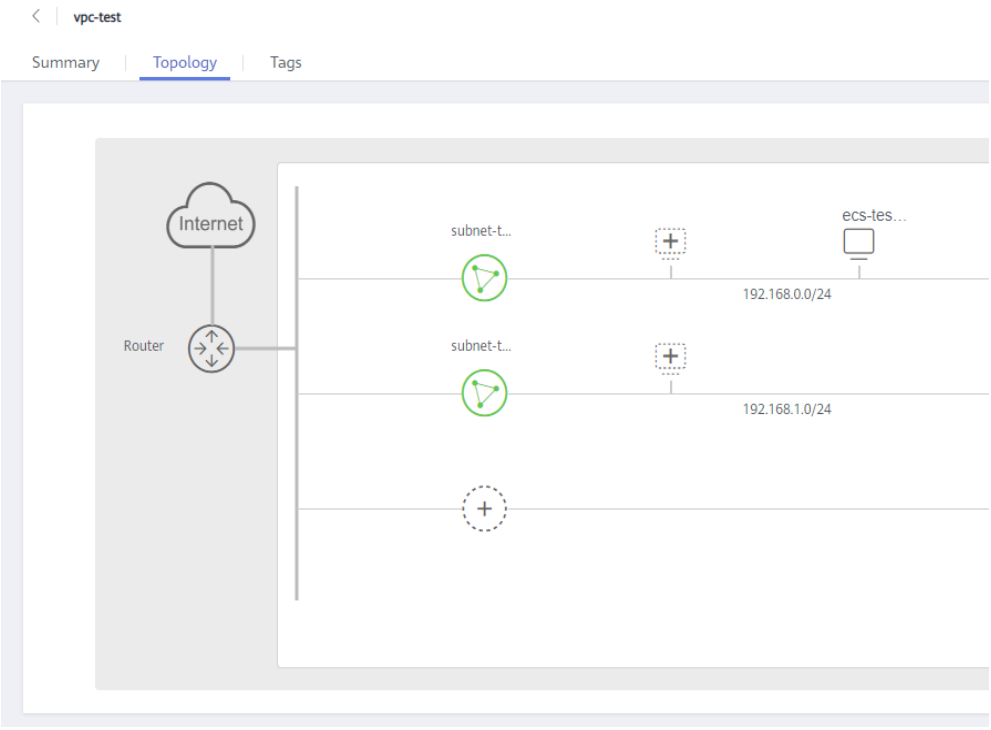
Scenarios

This section describes how to view the topology of a VPC. The topology displays the subnets in a VPC and the ECSs in the subnets.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. In the VPC list, click the name of the VPC for which the topology is to be viewed.
   The VPC details page is displayed.
5. Click the **Topology** tab to view the VPC topology.
   The topology displays the subnets in the VPC and the ECSs in the subnets.
   You can also perform the following operations on subnets and ECSs in the topology:
   – Modify or delete a subnet.
   – Add an ECS to a subnet, bind an EIP to the ECS, and change the security group of the ECS.

Figura 1-6 VPC topology



1.3 Subred

1.3.1 Creación de una subred para la VPC

Escenarios

Una VPC viene con una subred predeterminada. Si la subred predeterminada no puede cumplir sus requisitos, puede crear una.

La subred está configurada con DHCP de forma predeterminada. Cuando se inicia un ECS en esta subred, el ECS obtiene automáticamente una dirección IP mediante DHCP.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Subnets**.
5. Haga clic en **Create Subnet**.

   Se muestra la página **Create Subnet**.
6. Establezca los parámetros como se le solicite.

Tabla 1-7 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
VPC	VPC para la que desea crear una subred. Este parámetro sólo está disponible cuando **Subnets** se muestran en el panel de navegación.	-
AZ	Una AZ es una ubicación geográfica con fuente de alimentación independiente y instalaciones de red en una región. Las AZ están físicamente aisladas, y las AZ de la misma VPC están interconectadas a través de una red interna. Tenga en cuenta lo siguiente cuando seleccione una AZ: ● Una VPC puede tener las subredes que están en las diferentes AZ. Por ejemplo, una VPC puede tener una subred A en AZ 1, y una subred B en AZ 3. ● Un recurso en la nube y su subred pueden estar en las diferentes AZ. Por ejemplo, un servidor en la nube en AZ 1 puede usar una subred en AZ 3.	AZ1
Name	El nombre de la subred. El nombre puede contener un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios.	Subnet

Parámetro	Descripción	Valor de ejemplo
CIDR Block	El bloque CIDR para la subred. Este valor debe estar dentro del bloque CIDR de VPC. Este parámetro sólo se muestra en regiones donde no se admite la pila dual IPv4/IPv6.	192.168.0.0/24
IPv4 CIDR Block	El bloque CIDR para la subred. Este valor debe estar dentro del bloque CIDR de VPC. Este parámetro sólo se muestra en regiones donde se admite la doble pila IPv4/IPv6.	192.168.0.0/24
IPv6 CIDR Block	Especifica si se debe establecer **IPv6 CIDR Block** en **Enable**. Este parámetro sólo se muestra en regiones donde se admite la doble pila IPv4/IPv6. Si selecciona esta opción, el sistema asigna automáticamente un bloque CIDR IPv6 a la subred creada. Actualmente, el bloque CIDR IPv6 no se puede personalizar. La IPv6 no se puede deshabilitar después de haber creado la subred.	-
Associated Route Table	Tabla de rutas predeterminada a la que se asociará la subred. Puede cambiar la tabla de rutas a una tabla de rutas personalizada en la página **Subnets**.	Default
Advanced Settings/ Gateway	La dirección del gateway de la subred. Esta dirección IP se utiliza para comunicarse con otras subredes.	192.168.0.1
Advanced Settings/DNS Server Address	Las direcciones de servidor de DNS permiten que los ECS de una subred de VPC se comuniquen entre sí mediante nombres de dominio privados. También puede acceder directamente a los servicios en la nube a través de servidores DNS privados. Si desea utilizar otros servidores de DNS públicos para la resolución, puede cambiar las direcciones del servidor DNS predeterminado. También puede hacer clic en **Reset** a la derecha para restaurar las direcciones del servidor DNS al valor predeterminado. Se puede configurar un máximo de dos direcciones IP del servidor de DNS. Varias direcciones IP deben separarse mediante las comas (,).	100.125.x.x

Parámetro	Descripción	Valor de ejemplo
Advanced Settings/NTP Server Address	La dirección IP del servidor de NTP. Este parámetro es opcional. Puede configurar las direcciones IP del servidor de NTP para agregarse a la subred según sea necesario. Las direcciones IP se agregan además de las direcciones de servidor de NTP predeterminadas. Si este parámetro se deja vacío, no se agrega ninguna dirección IP del servidor NTP. Ingrese cuatro direcciones IP válidas como máximo y sepárelas con comas. Cada dirección IP debe ser única. Si agrega o cambia las direcciones del servidor de NTP de una subred, debe renovar la concesión DHCP o reiniciar todos los ECS de la subred para que el cambio surta efecto inmediatamente. Si las direcciones del servidor de NTP se han borrado, reiniciar los ECS no ayudará. Debe renovar la concesión DHCP para de todos los ECS para que el cambio se aplique inmediatamente.	192.168.2.1
Advanced Settings/ DHCP Lease Time	Período durante el cual un cliente puede utilizar una dirección IP asignada automáticamente por el servidor de DHCP. Una vez expirado el período de concesión, se asignará una nueva dirección IP al cliente. ● Limitado: Establezca el tiempo de concesión DHCP. La unidad puede ser de día u hora. ● Ilimitado: el tiempo de concesión DHCP no expira. Si se cambia el tiempo de la concesión DHCP, la nueva concesión se aplica automáticamente cuando ha pasado la mitad del tiempo de la concesión actual. Para aplicar el cambio inmediatamente, reinicie el ECS o acceda al ECS para generar la renovación automática de la concesión DHCP.	365 days
Advanced Settings/ Description	Información complementaria sobre la subred. Este parámetro es opcional. La descripción de la subred puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

7. Haga clic en **OK**.

Precauciones

Cuando se crea una subred, hay cinco direcciones IP reservadas, que no se pueden utilizar. Por ejemplo, en una subred con el bloque CIDR 192.168.0.0/24, se reservan las siguientes direcciones IP:

- 192.168.0.0: ID de red. Esta dirección es el comienzo del intervalo de direcciones IP privadas y no se asignará a ninguna instancia.
- 192.168.0.1: Dirección de gateway.
- 192.168.0.253: Reservado para la interfaz del sistema. Esta dirección IP es utilizada por la VPC para la comunicación externa.
- 192.168.0.254: Dirección del servicio DHCP.
- 192.168.0.255: Dirección de difusión de la red.

Si configuró la configuración predeterminada en **Advanced Settings** durante la creación de la subred, las direcciones IP reservadas pueden ser diferentes de las predeterminadas, pero todavía habrá cinco de ellas. Las direcciones específicas dependen de la configuración de subred.

1.3.2 Modificación de una subred

Escenarios

Modifique el nombre de subred, la dirección del servidor NTP y la dirección del servidor de DNS. No se puede modificar la AZ de una subred creada.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
5. Busque la fila que contiene la VPC de destino y haga clic en el número en la columna **Subnets**.

   Se muestra la página **Subnets**.
6. En la lista de subred, busque la subred de destino y haga clic en su nombre.

   Se muestra la página de detalles de subred.
7. En la ficha **Summary**, haga clic en  a la derecha del parámetro que se va a modificar y modifique el parámetro según se le solicite.

Tabla 1-8 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	El nombre de la subred. El nombre puede contener un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios.	Subnet
DNS Server Address	Las direcciones de servidor de DNS permiten que los ECS de una subred de VPC se comuniquen entre sí mediante nombres de dominio privados. También puede acceder directamente a los servicios en la nube a través de servidores DNS privados. Si desea utilizar otros servidores de DNS públicos para la resolución, puede cambiar las direcciones del servidor DNS predeterminado. También puede hacer clic en **Reset** a la derecha para restaurar las direcciones del servidor DNS al valor predeterminado. Se puede configurar un máximo de dos direcciones IP del servidor de DNS. Varias direcciones IP deben separarse mediante las comas (,).	100.125.x.x

Parámetro	Descripción	Valor de ejemplo
DHCP Lease Time	Período durante el cual un cliente puede utilizar una dirección IP asignada automáticamente por el servidor de DHCP. Una vez expirado el período de concesión, se asignará una nueva dirección IP al cliente. ● Limitado: Establezca el tiempo de concesión DHCP. La unidad puede ser de día u hora. ● Ilimitado: el tiempo de concesión DHCP no expira. Si se cambia el tiempo de la concesión DHCP, la nueva concesión se aplica automáticamente cuando ha pasado la mitad del tiempo de la concesión actual. Para aplicar el cambio inmediatamente, reinicie el ECS o acceda al ECS para generar la renovación automática de la concesión DHCP.	365 days

Parámetro	Descripción	Valor de ejemplo
NTP Server Address	La dirección IP del servidor de NTP. Este parámetro es opcional. Puede configurar las direcciones IP del servidor de NTP para agregarse a la subred según sea necesario. Las direcciones IP se agregan además de las direcciones de servidor de NTP predeterminadas. Si este parámetro se deja vacío, no se agrega ninguna dirección IP del servidor NTP. Ingrese cuatro direcciones IP válidas como máximo y sepárelas con comas. Cada dirección IP debe ser única. Si agrega o cambia las direcciones del servidor de NTP de una subred, debe renovar la concesión DHCP o reiniciar todos los ECS de la subred para que el cambio surta efecto inmediatamente. Si las direcciones del servidor de NTP se han borrado, reiniciar los ECS no ayudará. Debe renovar la concesión DHCP para de todos los ECS para que el cambio se aplique inmediatamente.	192.168.2.1
Description	Información complementaria sobre la subred. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

8. Haga clic en **OK**.

1.3.3 Gestión de etiquetas de subred

Escenarios

Una etiqueta de subred identifica una subred. Las etiquetas se pueden agregar a las subredes para facilitar la identificación y gestión de las subredes. Puede agregar una etiqueta a una subred al crear la subred, o puede agregar una etiqueta a una subred creada en la página de detalles de la subred. Se puede agregar un máximo de 10 etiquetas a cada subred.

Una etiqueta consiste en un par clave y valor. **Tabla 1-9** enumera los requisitos de valor y clave de etiqueta.

Tabla 1-9 Clave de etiqueta de subred y requisitos de valor

Parámetro	Requerimientos	Valor de ejemplo
Key	● No se puede dejar en blanco. ● Debe ser único para cada subred. ● Puede contener un máximo de 36 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), y guiones (-).	subnet_key1
Value	● Puede contener un máximo de 43 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), puntos (.) y guiones (-).	subnet-01

Procedimiento

Busque subredes por la clave de etiqueta y el valor en la página que muestra la lista de subredes.

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
5. Busque la fila que contiene la VPC de destino y haga clic en el número en la columna **Subnets**.

   Se muestra la página **Subnets**.
6. En la esquina superior derecha de la lista de subred, haga clic en **Search by Tag**.
7. Introduzca la clave de etiqueta de la subred que se va a consultar.

   Se deben especificar tanto la clave de etiqueta como el valor. El sistema muestra automáticamente las subredes que está buscando si coinciden tanto la clave de etiqueta como el valor.
8. Haga clic en + para agregar otra clave y valor de etiqueta.

   Se pueden agregar múltiples claves y valores de etiquetas para restringir los resultados de la búsqueda. Si agrega más de una etiqueta a la búsqueda de subredes, se mostrarán las subredes que contienen todas las etiquetas especificadas.
9. Haga clic en **Search**.

   El sistema muestra las subredes que está buscando en función de las claves de etiqueta y los valores introducidos.

Agregar, eliminar, editar y ver etiquetas en la ficha Tags de una subred.

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

3. En **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
5. Busque la fila que contiene la VPC de destino y haga clic en el número en la columna **Subnets**.

   Se muestra la página **Subnets**.
6. En la lista de subred, busque la subred de destino y haga clic en su nombre.
7. En la página de detalles de subred, haga clic en la ficha **Tags** y realice las operaciones deseadas en las etiquetas.
   - Consulte etiquetas.

     En la ficha **Tags**, puede ver detalles sobre las etiquetas agregadas a la subred actual, incluido el número de etiquetas y la clave y el valor de cada etiqueta.
   - Agregue una etiqueta.

     Haga clic en **Add Tag** en la esquina superior izquierda. En el cuadro de diálogo **Add Tag** que se muestra, escriba la clave y el valor de la etiqueta y haga clic en **OK**.
   - Edite una etiqueta.

     Busque la fila que contiene la etiqueta que desea editar y haga clic en **Edit** en la columna **Operation**. En el cuadro de diálogo **Edit Tag**, cambie el valor de la etiqueta y haga clic en **OK**.
   - Elimine una etiqueta.

     Busque la fila que contiene la etiqueta que desea eliminar y haga clic en **Delete** en la columna **Operation**. En la caja de diálogo que aparece, haga clic en **Yes**.

1.3.4 Exporting Subnet List

Scenarios

Information about all subnets under your account can be exported as an Excel file to a local directory. This file records the name, ID, VPC, CIDR block, and associated route table of each subnet.

Procedure

1. Log in to the management console.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Under **Networking**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Subnets**.
5. In the upper right corner of the subnet list, click  .

   The system will automatically export information about all subnets under your account in the current region as an Excel file to a local directory.

1.3.5 Supresión de una subred

Escenarios

Puede eliminar una subred para liberar recursos de red si la subred ya no es necesaria.

Prerrequisitos

Puede eliminar una subred sólo si no hay recursos en la subred. Si hay recursos en la subred, debe eliminarlos antes de poder eliminar la subred.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Virtual Private Cloud**.
5. Busque la fila que contiene la VPC de destino y haga clic en el número en la columna **Subnets**.

   Se muestra la página **Subnets**.
6. En la lista de subred, busque la fila que contiene la subred que desea eliminar y haga clic en **Delete** en la columna **Operation**.

   Aparecerá en pantalla un cuadro de diálogo de confirmación.
7. Haga clic en **Yes**.

1.4 Red de doble pila IPv4 e IPv6

¿Qué es una red de doble pila IPv4/IPv6?

La doble pila IPv4 e IPv6 permite que sus recursos, como los ECS, utilicen las direcciones IPv4 e IPv6 para comunicaciones de las redes públicas y las privadas. Por ejemplo, si los ECS utilizan la red de doble pila IPv4/IPv6:

- Los ECS pueden comunicarse entre sí mediante las direcciones IPv4 privadas.
- Los ECS pueden comunicarse con Internet después de estar vinculados con las EIP.
- Los ECS pueden comunicarse entre sí mediante las direcciones IPv6.
- Los ECS pueden comunicarse con Internet después de que sus direcciones IPv6 estén asociadas con anchos de banda.

NOTA

Si selecciona **Enable** para **IPv6 CIDR Block** al crear una subred, se asignará automáticamente un bloque CIDR IPv6 a la subred.

Las operaciones básicas en redes de doble pila IPv4 e IPv6 son las mismas que en redes IPv4, excepto algunos parámetros. Consulte las páginas de la consola para obtener más información.

Notas y restricciones

- La función de doble pila IPv4/IPv6 es actualmente gratuita, pero se facturará en una fecha posterior (el precio aún no se ha determinado).
- Solo las variantes ECS que admiten las direcciones IPv6 pueden utilizar las redes de doble pila IPv4/IPv6.

  Puede utilizar cualquiera de los siguientes métodos para comprobar qué variantes de ECS admiten las direcciones IPv6:

  – En la consola de ECS, haga clic en **Buy ECS**. En la página mostrada, vea las variantes de ECS.

    Si una variante de ECS tiene el parámetro **IPv6** con el valor **Yes**, la variante de ECS admite las direcciones IPv6.

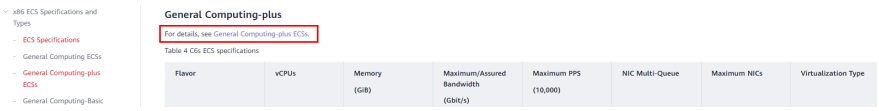
  – En la página de **especificaciones de ECS**, haga clic en el enlace de las especificaciones de ECS deseadas para obtener la información detallada y compruebe las variantes de ECS que admiten IPv6 en la tabla de características de ECS.

    Por ejemplo, si desea comprobar las variantes de los ECS de cómputo-plus que admiten IPv6:

    i. Abra la página **Especificaciones de ECS**.

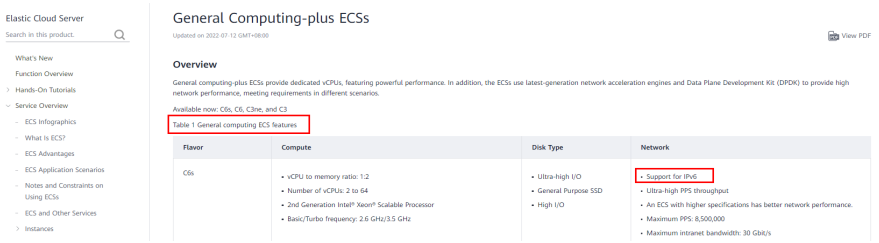
    ii. En **General Computing-Plus**, haga clic en el enlace para obtener información detallada.

    Figura 1-7 Enlace para la información detallada

    iii. En la página **General Computing-plus ECSs**, compruebe si IPv6 es compatible en la tabla de características de ECS.

    Figura 1-8 ECS de cómputo-plus

Escenarios de aplicaciones de IPv6

Si su ECS admite IPv6, puede utilizar la red de doble pila IPv4/IPv6. **Tabla 1-10** muestra los escenarios de aplicación de ejemplo.

Tabla 1-10 Escenarios de aplicación de doble pila IPv4/IPv6

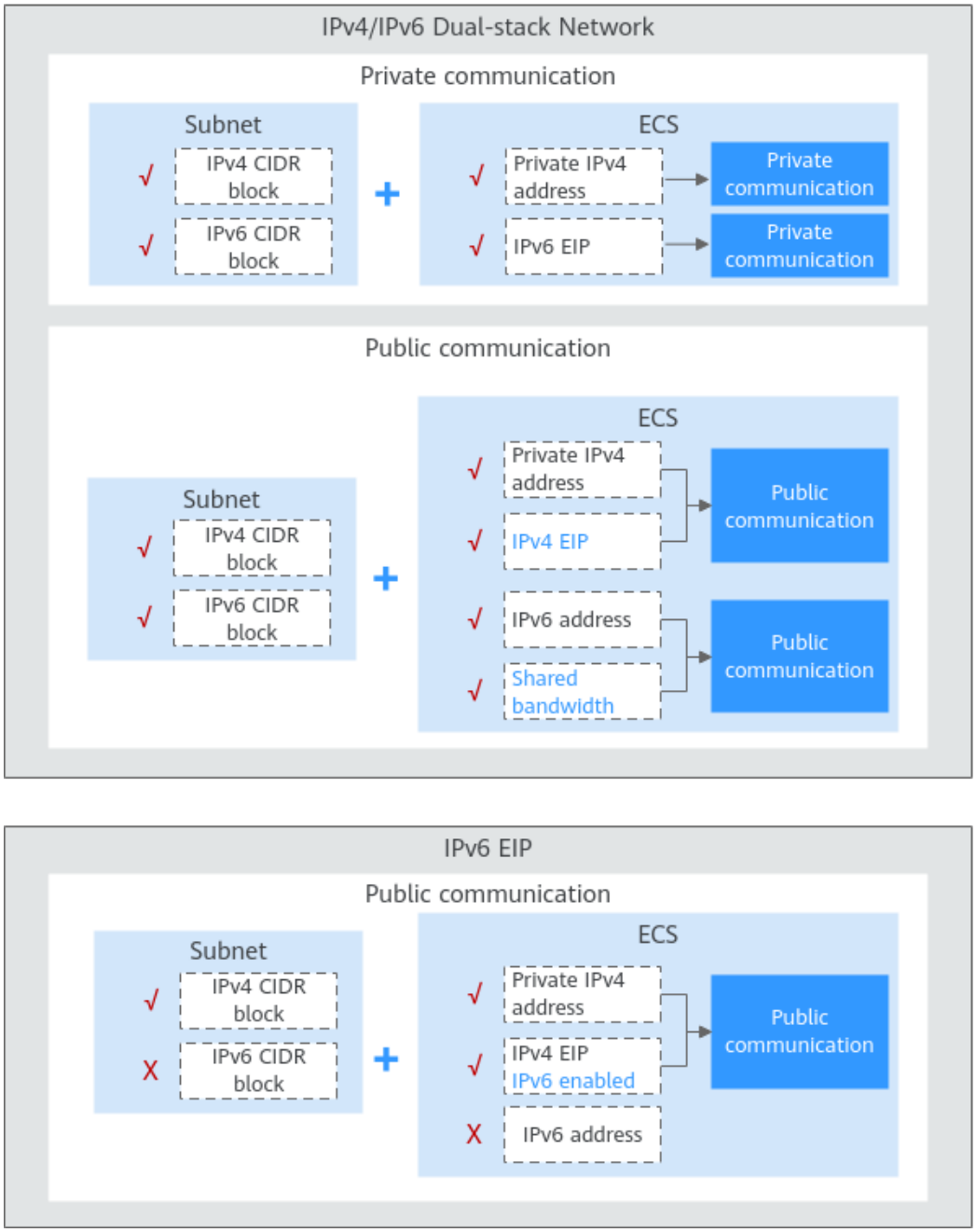
Escenario de la aplicación	Descripción	Subred	ECS
Comunicación privada mediante las direcciones IPv6	Las aplicaciones implementadas en ECS deben comunicarse con otros sistemas (como bases de datos) a través de redes privadas mediante direcciones IPv6.	● Bloque CIDR IPv4 ● Bloque CIDR IPv6	● Dirección IPv4 privada: utilizada para la comunicación privada ● Dirección IPv6: utilizada para la comunicación privada.
Comunicación pública mediante direcciones IPv6	Las aplicaciones implementadas en ECS deben proporcionar servicios accesibles desde Internet mediante direcciones IPv6.	● Bloque CIDR IPv4 ● Bloque CIDR IPv6	● Dirección IPv4 privada + IPv4 EIP: utilizada para la comunicación de redes públicas ● Dirección IPv6 + ancho de banda compartido: utilizado para la comunicación de red pública
	Sus aplicaciones implementadas en ECS deben proporcionar servicios accesibles desde Internet y analizar los datos de solicitud de acceso mediante direcciones IPv6.		

Si su variante de ECS no admite las direcciones IPv6, puede habilitar la función IPv6 EIP para permitir comunicaciones mediante direcciones IPv6. Para más detalles, consulte **Tabla 1-11**.

Tabla 1-11 Escenarios de aplicación de EIP IPv6

Escenario de la aplicación	Descripción	Subred	ECS
Comunicación pública mediante direcciones IPv6	Las aplicaciones implementadas en ECS deben proporcionar servicios accesibles desde Internet mediante direcciones IPv6.	Bloque CIDR IPv4	● Dirección IPv4 privada ● IPv4 EIP (con función IPv6 habilitada): se utiliza para la comunicación pública mediante las EIP de IPv4 y de IPv6

Figura 1-9 Escenarios de aplicación de redes IPv6



Operaciones básicas

Creación de una subred IPv6

Cree una subred IPv6 siguiendo las instrucciones en **Creación de una subred para la VPC**. Seleccione **Enable** para **IPv6 CIDR Block**. Un bloque CIDR IPv6 se asignará automáticamente a la subred. La IPv6 no se puede deshabilitar después de haber creado la subred. Actualmente, no se admite la personalización del bloque CIDR IPv6.

Consulta de direcciones IPv6 en uso

En la lista de subred, haga clic en el nombre de la subred. En la página mostrada, vea las direcciones IPv6 en uso en la página de ficha **IP Addresses**.

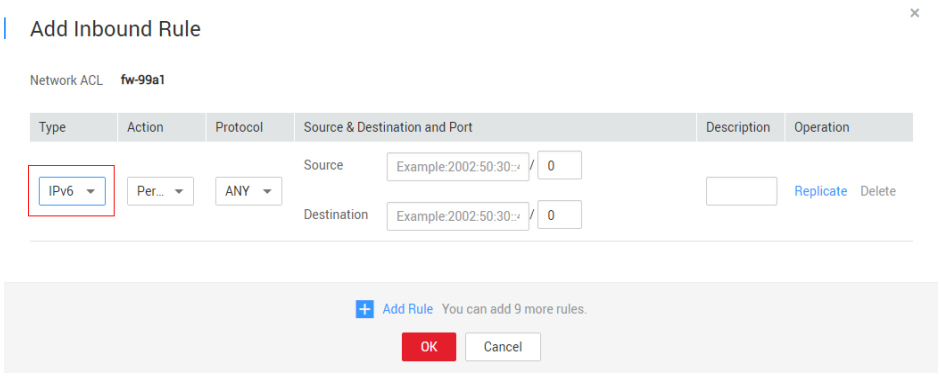
Adición de una regla de grupo de seguridad (IPv6)

Agregue una regla de grupo de seguridad con **Type** establecido en **IPv6** y el **Source** o **Destination** establecido en una dirección IPv6 o un bloque CIDR IPv6.

Adición de una regla de ACL de red (IPv6)

Agregue una regla de ACL de red con **Type** establecido en **IPv6** y el **Source** o **Destination** establecido en una dirección IPv6 o un bloque CIDR IPv6.

Figura 1-10 Adición de una regla de ACL de red (IPv6)



Adición de una ruta (IPv6)

Agregue una ruta con **Destination** y **Next Hop** configurados en un bloque CIDR IPv4 o IPv6. Para obtener más información sobre cómo agregar una ruta, consulte **Adición de una ruta personalizada**. Si el destino es un bloque CIDR IPv6, el salto siguiente solo puede ser una dirección IP en la misma VPC que el bloque CIDR IPv6.

NOTA

Si el destino es un bloque CIDR IPv6, el tipo de salto siguiente solo puede ser un ECS, una NIC de extensión o una dirección IP virtual. El salto siguiente también debe tener direcciones IPv6.

Asignación dinámica de las direcciones IPv6

Una vez creado correctamente un ECS, puede ver la dirección IPv6 asignada en la página de detalles de ECS. También puede iniciar sesión en ECS y ejecutar el comando **ifconfig** para ver la dirección IPv6 asignada.

Si una dirección IPv6 no se asigna automáticamente o la imagen seleccionada no admite la función de asignación automática de direcciones IPv6, obtener manualmente la dirección IPv6 haciendo referencia a **Asignar dinámicamente las direcciones de 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.

2 Seguridad

2.1 Grupo de seguridad

2.1.1 Aspectos generales de los grupos de seguridad

Grupo de seguridad

Un grupo de seguridad es una colección de reglas de control de acceso para recursos en la nube, como servidores en la nube, contenedores y bases de datos, que tienen los mismos requisitos de protección de seguridad y que son de confianza mutua dentro de una VPC. Después de crear un grupo de seguridad, puede crear varias reglas de acceso para el grupo de seguridad, estas reglas se aplicarán a todos los recursos de nube agregados a este grupo de seguridad.

Su cuenta viene automáticamente con un grupo de seguridad predeterminado. El grupo de seguridad predeterminado permite todo el tráfico saliente, niega todo el tráfico entrante y permite todo el tráfico entre los recursos de nube del grupo. Sus recursos en la nube de este grupo de seguridad ya pueden comunicarse entre sí sin agregar reglas adicionales. Puede utilizar directamente el grupo de seguridad predeterminado. Para más detalles, consulte **Grupos de seguridad predeterminados y reglas de grupos de seguridad**.

También puede crear grupos de seguridad personalizados para satisfacer sus requisitos de servicio específicos. Para más detalles, consulte **Creación de un grupo de seguridad**.

Conceptos básicos del grupo de seguridad

- Puede asociar las instancias, como servidores y NIC de extensión, con uno o más grupos de seguridad.

  Puede cambiar los grupos de seguridad asociados a instancias, como servidores o NIC de extensión. De forma predeterminada, al crear una instancia, se asocia con el grupo de seguridad predeterminado de su VPC a menos que especifique otro grupo de seguridad.
- Debe agregar reglas de grupo de seguridad para permitir que las instancias del mismo grupo de seguridad se comuniquen entre sí.
- Los grupos de seguridad son de estado. Si envía una solicitud desde la instancia y se permite el tráfico saliente, el tráfico de respuesta para esa solicitud puede fluir

independientemente de las reglas del grupo de seguridad entrante. De manera similar, si se permite el tráfico entrante, se permite que las respuestas al tráfico entrante permitido fluyan hacia fuera, independientemente de las reglas salientes.

Los grupos de seguridad utilizan el seguimiento de conexión para realizar un seguimiento del tráfico hacia y desde las instancias que contienen y las reglas de grupo de seguridad se aplican en función del estado de conexión del tráfico para determinar si se permite o se deniega el tráfico. Si agrega, modifica o elimina una regla de grupo de seguridad, o crea o elimina una instancia en el grupo de seguridad, el seguimiento de conexión de todas las instancias del grupo de seguridad se borrará automáticamente. En este caso, el tráfico entrante o saliente de la instancia se considerará como nuevas conexiones, que deben coincidir con las reglas de grupo de seguridad entrante o saliente para garantizar que las reglas entren en vigor inmediatamente y la seguridad del tráfico entrante.

Además, si el tráfico entrante o saliente de una instancia no tiene paquetes durante mucho tiempo, el tráfico se considerará como nuevas conexiones después de que el seguimiento de la conexión se agote, y las conexiones deben coincidir con las reglas saliente e entrante. El periodo de tiempo de espera del seguimiento de la conexión varía según el protocolo. El periodo de tiempo de espera de una conexión TCP en el estado establecido es 600s, y el periodo de tiempo de espera de una conexión ICMP es 30s. Para otros protocolos, si se reciben paquetes en ambas direcciones, el periodo de tiempo de espera de seguimiento de conexión es de 180 segundos. Si se reciben uno o más paquetes en una dirección pero no se recibe ningún paquete en la otra dirección, el período de tiempo de espera de seguimiento de conexión es de 30 segundos. Para los protocolos distintos de TCP, UDP e ICMP, solo se realiza un seguimiento de la dirección IP y el número de protocolo.

NOTA

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 un interconexión de VPC para conectar los dos VPC.

Reglas de grupos de seguridad

Después de crear un grupo de seguridad, puede agregar reglas al grupo de seguridad. Una regla se aplica al tráfico entrante o al tráfico saliente. Después de agregar recursos de nube al grupo de seguridad, están protegidos por las reglas del grupo.

Una regla de grupo de seguridad consta de:

- **Source** (regla de entrada) o **Destination** (regla de salida): El valor puede ser una dirección IP (como 192.168.10.10/32), un rango de direcciones IP (como 192.168.52.0/24), o un grupo de seguridad (como sg-abc).
- **Protocol & Port**: El valor de los puertos puede ser puertos individuales (como 22), puertos consecutivos (como 22-30), puertos y rangos de puertos (como 20,23-30), todos los puertos (1-65535). El protocolo puede ser TCP, UDP, HTTP y otros.
- **Source**: el valor puede ser una única dirección IP, un grupo de direcciones IP, o un grupo de seguridad.
- **Type**: El valor puede ser IPv4 o IPv6.
- **Description**: Información complementaria sobre la regla de grupo de seguridad.

Cada grupo de seguridad tiene sus reglas predeterminadas. Para más detalles, consulte **Tabla 2-2**. También puede personalizar las reglas del grupo de seguridad. Para más detalles, consulte **Adición de una regla de grupo de seguridad**.

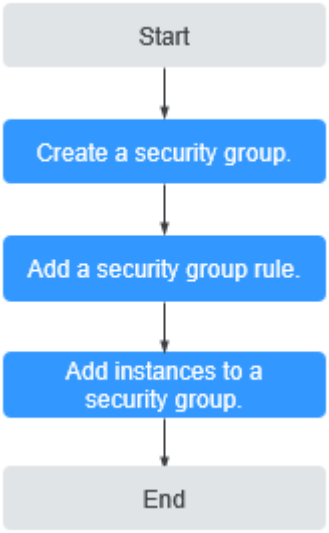
Plantilla de grupo de seguridad

Puede seleccionar una de las siguientes plantillas de grupo de seguridad proporcionadas por el sistema para crear rápidamente un grupo de seguridad con reglas predeterminadas.

- **General-purpose web server**: el grupo de seguridad que se crea con esta plantilla es para servidores web de propósito general e incluye reglas predeterminadas que permiten todo el tráfico ICMP entrante y el tráfico entrante en los puertos 22, 80, 443 y 3389.
- **All ports open**: el grupo de seguridad que cree con esta plantilla incluye reglas predeterminadas que permiten el tráfico entrante en cualquier puerto. Tenga en cuenta que permitir el tráfico entrante en cualquier puerto plantea riesgos de seguridad.
- **Custom**: el grupo de seguridad que cree con esta plantilla incluye reglas predeterminadas que deniegan el tráfico entrante en cualquier puerto. Puede agregar o modificar reglas de grupo de seguridad según sea necesario.

Proceso de configuración del grupo de seguridad

Figura 2-1 Proceso para configurar un grupo de seguridad



Restricciones del grupo de seguridad

- De forma predeterminada, puede crear un máximo de 100 grupos de seguridad en su cuenta en la nube.
- De forma predeterminada, puede agregar hasta 50 reglas de grupo de seguridad a un grupo de seguridad.
- De forma predeterminada, no puede asociar más de cinco grupos de seguridad a cada ECS o NIC de extensión. En tal caso, las reglas de todos los grupos de seguridad seleccionados se agregan para que surtan efecto.
- Si un servidor en la nube o una NIC de extensión están asociados a varios grupos de seguridad, las reglas de grupo de seguridad se aplicarán según la siguiente secuencia: el primer grupo de seguridad asociado tendrá prioridad sobre los asociados más tarde, luego la regla con la prioridad más alta en ese grupo de seguridad se aplicará primero.
- Puede agregar un máximo de 20 instancias a un grupo de seguridad a la vez.

- No agregue más de 1000 instancias al mismo grupo de seguridad. De lo contrario, el rendimiento del grupo de seguridad puede verse afectado.
- Las reglas de grupo de seguridad con ciertas configuraciones no tienen efecto para los ECS de ciertas especificaciones. **Tabla 2-1** muestra los detalles.

Tabla 2-1 Escenarios en los que las reglas del grupo de seguridad no entran en vigor

Configuración de regla	Tipo de ECS
• **Action** se establece en **Deny**. • **Source** o **Destination** se establece en **IP address group**.	No se admiten los siguientes tipos de ECS x86: • Memoria optimizada (ECS M1) • Cómputo de alto rendimiento (ECS H1) • Intensivo de disco (ECS D1) • Acelerada por GPU (ECS G1 y G2) • Memoria grande (ECS E1, E2 y ET2)
Port se establece en puertos no consecutivos.	No se admiten los siguientes tipos de ECS x86: • Cómputo general (ECS S1, C1 y C2) • Memoria optimizada (ECS M1) • Cómputo de alto rendimiento (ECS H1) • Intensivo de disco (ECS D1) • Acelerada por GPU (ECS G1 y G2) • Memoria grande (ECS E1, E2 y ET2)
	No se admiten todos los ECS de Kunpeng.

Sugerencias

Cuando se utiliza un grupo de seguridad:

- No agregue todas las instancias al mismo grupo de seguridad si tienen requisitos de aislamiento diferentes.
- No es necesario que cree un grupo de seguridad para cada instancia. En su lugar, puede agregar instancias con los mismos requisitos de seguridad al mismo grupo de seguridad.

Al agregar una regla de grupo de seguridad:

- Definir reglas de grupo de seguridad simples. Por ejemplo, si agrega una instancia a varios grupos de seguridad, la instancia puede cumplir con cientos de reglas de grupo de seguridad y un cambio en cualquier regla puede provocar la desconexión de la red para la instancia.
- Antes de modificar un grupo de seguridad y sus reglas, clone el grupo de seguridad y, a continuación, modifique el grupo de seguridad clonado para probar la comunicación y evitar efectos adversos en los servicios en ejecución.
- Al agregar una regla de grupo de seguridad para una instancia, conceda los permisos mínimos posibles. Por ejemplo:
  - Abra un puerto específico, por ejemplo, 22. No se recomienda abrir un rango de puertos, por ejemplo, 22-30.

  - No se recomienda que introduzca 0.0.0.0/0, permitiendo el tráfico hacia o desde todas las direcciones IP.

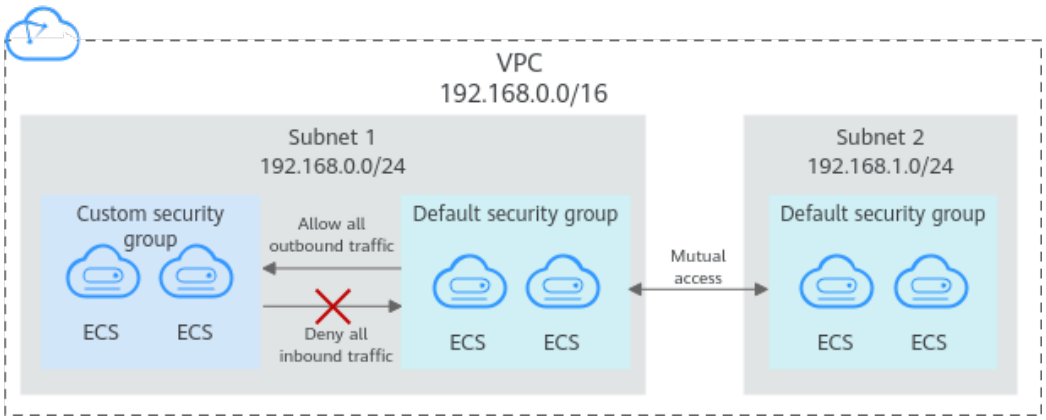
- Una regla de grupo de seguridad entra en vigor inmediatamente para sus ECS asociados después de configurar la regla sin reiniciar ECS. Independientemente de las reglas entrantes de un grupo de seguridad, se permite el tráfico de respuesta del tráfico saliente.

2.1.2 Grupos de seguridad predeterminados y reglas de grupos de seguridad

Su cuenta viene automáticamente con un grupo de seguridad predeterminado (**Sys-default**). El grupo de seguridad predeterminado permite todo el tráfico saliente, niega todo el tráfico entrante y permite todo el tráfico entre los recursos de nube del grupo. Sus recursos en la nube de este grupo de seguridad ya pueden comunicarse entre sí sin agregar reglas adicionales.

Figura 2-2 muestra las reglas de grupo de seguridad predeterminadas. A continuación se utiliza el acceso entre ECS como ejemplo.

Figura 2-2 Grupo de seguridad predeterminado



NOTA

- No se puede eliminar el grupo de seguridad predeterminado, pero se pueden modificar las reglas para el grupo de seguridad predeterminado.
- 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 un interconexión de VPC para conectar los dos VPC. Para obtener más información acerca de la conectividad de VPC, consulte **Escenarios de aplicaciones**.

Tabla 2-2 describe las reglas predeterminadas para el grupo de seguridad predeterminado (**Sys-default**).

Tabla 2-2 Reglas en el grupo de seguridad predeterminado (**Sys-default**)

Dirección	Prioridad	Acción	Protocolo	Puerto/Rango	Origen/Destino	Descripción
Saliente	100	Permitir	Todos	Todos	Destino: 0.0.0.0/0	Permite todo el tráfico de salida.

Dirección	Prioridad	Acción	Protocolo	Puerto/Rango	Origen/Destino	Descripción
Entrante	100	Permitir	Todos	Todos	Origen: el grupo de seguridad actual, por ejemplo, **Sys-default**	Permite las comunicaciones entre ECS dentro del mismo grupo de seguridad en cualquier puerto.
Entrante	100	Permitir	TCP	22	Origen: 0.0.0.0/0	Permite que todas las direcciones IP accedan a los ECS Linux mediante SSH.
Entrante	100	Permitir	TCP	3389	Origen: 0.0.0.0/0	Permite que todas las direcciones IP accedan a ECS de Windows a través de RDP.

2.1.3 Ejemplos de configuración de grupo de seguridad

Las configuraciones comunes de grupos de seguridad se presentan aquí. Los ejemplos de esta sección permiten todos los paquetes de datos salientes de forma predeterminada. Esta sección solo describirá cómo configurar reglas entrantes.

- **Permitir el acceso externo a un puerto especificado**
- **Habilitación de ECS en diferentes grupos de seguridad para comunicarse entre sí a través de una red interna**
- **Habilitación de direcciones IP especificadas para acceder de forma remota a ECS en un grupo de seguridad**
- **Conectarse de forma remota a ECS Linux mediante SSH**
- **Conectarse de forma remota a ECS Windows mediante RDP**
- **Habilitación de la comunicación entre ECS**
- **Alojamiento de un sitio web en ECS**
- **Cómo habilitar un ECS para que funcione como servidor DNS.**
- **Carga o descarga de archivos que usan FTP**

Puede utilizar el grupo de seguridad predeterminado o crear un grupo de seguridad por adelantado. Para obtener más información, consulte las secciones **Creación de un grupo de seguridad** y **Adición de una regla de grupo de seguridad**.

Permitir el acceso externo a un puerto especificado

- Ejemplo del escenario:

  Después de implementar los servicios, puede agregar reglas de grupo de seguridad para permitir el acceso externo a un puerto especificado (por ejemplo, 1100).
- Regla del grupo de seguridad:

Dirección	Protocolo	Puerto	Fuente
Entrante	TCP	1100	0.0.0.0/0

Habilitación de ECS en diferentes grupos de seguridad para comunicarse entre sí a través de una red interna

- Ejemplo del escenario:

  Los recursos de un ECS de un grupo de seguridad deben copiarse en un ECS asociado con otro grupo de seguridad. Los dos ECS están en la misma VPC. Se recomienda habilitar la comunicación de la red privada entre los ECS y, a continuación, copiar los recursos.

- Configuración del grupo de seguridad:

  Dentro de una VPC dada, los ECS del mismo grupo de seguridad pueden comunicarse entre sí de forma predeterminada. Sin embargo, los ECS de diferentes grupos de seguridad no pueden comunicarse entre sí por defecto. Para permitir que estos ECS se comuniquen entre sí, debe agregar ciertas reglas de grupo de seguridad.

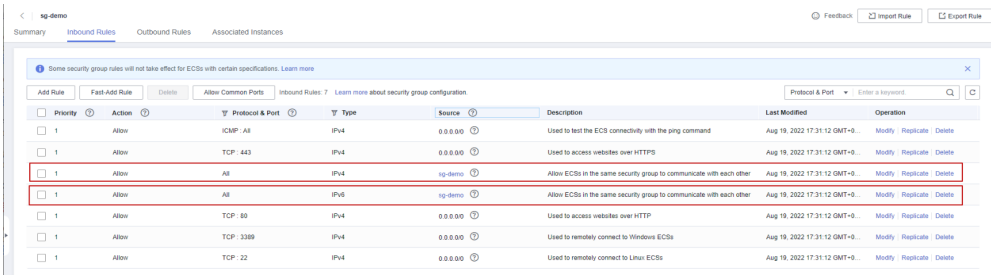
  Puede agregar una regla entrante a los grupos de seguridad que contienen los ECS para permitir el acceso desde los ECS del otro grupo de seguridad. La regla requerida es la siguiente.

Dirección	Protocolo/Aplicación	Puerto	Fuente
Entrante	Utilizado para la comunicación a través de una red interna	Puerto o rango de puertos	ID de otro grupo de seguridad

AVISO

Si los ECS asociados con el mismo grupo de seguridad no pueden comunicarse entre sí, compruebe si se ha eliminado la regla que permite la comunicación.

A continuación se utiliza el grupo de seguridad **sg-demo** como ejemplo. La regla con **Source** establecida en **sg-demo** permite que los recursos asociados con este grupo de seguridad se comuniquen entre sí.



Habilitación de direcciones IP especificadas para acceder de forma remota a ECS en un grupo de seguridad

- Ejemplo del escenario:

  Para evitar que los ECS sean atacados, puede cambiar el puerto para el inicio de sesión remoto y configurar reglas de grupo de seguridad que permiten que solo las direcciones IP especificadas accedan de forma remota a los ECS.

- Configuración del grupo de seguridad:

  Para permitir que la dirección IP **192.168.20.2** acceda de forma remota a los ECS de Linux en un grupo de seguridad a través del protocolo SSH (puerto 22), puede configurar la siguiente regla de grupo de seguridad.

Dirección	Protocolo	Puerto	Fuente
Entrante	SSH	22	Bloque CIDR IPv4 o ID de otro grupo de seguridad Por ejemplo, 192.168.20.2/32

Conectarse de forma remota a ECS Linux mediante SSH

- Ejemplo del escenario:

  Después de crear los ECS de Linux, puede agregar una regla de grupo de seguridad para habilitar el acceso SSH remoto a los ECS.

  NOTA

  El grupo de seguridad predeterminado viene con la siguiente regla. Si utiliza el grupo de seguridad predeterminado, no es necesario volver a agregar esta regla.

- Regla del grupo de seguridad:

Dirección	Protocolo	Puerto	Fuente
Entrante	SSH	22	0.0.0.0/0

Conectarse de forma remota a ECS Windows mediante RDP

- Ejemplo del escenario:

  Después de crear los ECS de Windows, puede agregar una regla de grupo de seguridad para habilitar el acceso remoto de RDP a los ECS.

  NOTA

  El grupo de seguridad predeterminado viene con la siguiente regla. Si utiliza el grupo de seguridad predeterminado, no es necesario volver a agregar esta regla.

- Regla del grupo de seguridad:

Dirección	Protocolo	Puerto	Fuente
Entrante	RDP	3389	0.0.0.0/0

Habilitación de la comunicación entre ECS

- Ejemplo del escenario:

  Después de crear los ECS, debe agregar una regla de grupo de seguridad para que pueda ejecutar el comando **ping** para probar la comunicación entre los ECS.

- Regla del grupo de seguridad:

Dirección	Protocolo	Puerto	Fuente
Entrante	ICMP	Todos	0.0.0.0/0

Alojamiento de un sitio web en ECS

- Ejemplo del escenario:

  Si implementa un sitio web en sus ECS y requiere que se acceda a su sitio web a través de HTTP o HTTPS, puede agregar reglas al grupo de seguridad utilizado por los ECS que funcionan como servidores web.

- Regla del grupo de seguridad:

Dirección	Protocolo	Puerto	Fuente
Entrante	HTTP	80	0.0.0.0/0
Entrante	HTTPS	443	0.0.0.0/0

Cómo habilitar un ECS para que funcione como servidor DNS.

- Ejemplo del escenario:

  Si necesita utilizar un ECS como un servidor de DNS, debe permitir el acceso TCP y UDP desde el puerto 53 al servidor de DNS. Puede agregar las siguientes reglas al grupo de seguridad asociado al ECS.

- Reglas del grupo de seguridad:

Dirección	Protocolo	Puerto	Fuente
Entrante	TCP	53	0.0.0.0/0
Entrante	UDP	53	0.0.0.0/0

Carga o descarga de archivos que usan FTP

- Ejemplo del escenario:

Si desea utilizar el protocolo de transferencia de archivos (FTP) para cargar o descargar archivos de ECS, debe agregar una regla de grupo de seguridad.

NOTA

Instale primero el programa del servidor FTP en los ECS y verifique si los puertos 20 y 21 están funcionando correctamente.

- Regla del grupo de seguridad:

Dirección	Protocolo	Puerto	Fuente
Entrante	TCP	20-21	0.0.0.0/0

Adición de un ECS a varios grupos de seguridad

Es posible que deba agregar un ECS a varios grupos de seguridad según los requisitos del servicio. Las reglas del grupo de seguridad se aplicarán según la siguiente secuencia: el primer grupo de seguridad asociado tendrá prioridad sobre los asociados más tarde, luego la regla con la prioridad más alta en ese grupo de seguridad se aplicará primero. El uso de varios grupos de seguridad puede causar problemas al acceder a ECS. Le recomendamos que no asocie más de cinco grupos de seguridad a cada ECS.

2.1.4 Creación de un grupo de seguridad

Escenarios

Puede crear un grupo de seguridad y agregar ECS en una VPC al grupo de seguridad para mejorar la seguridad del acceso a ECS. Le recomendamos que asigne ECS que tengan diferentes políticas de acceso a Internet a diferentes grupos de seguridad.

Cada ECS debe estar asociado con al menos un grupo de seguridad. Si no tiene grupos de seguridad al comprar un ECS, el ECS utilizará el **grupo de seguridad predeterminado** (Sys-default).

Tiene la opción de crear un nuevo grupo de seguridad para el ECS. Esta sección describe cómo crear un grupo de seguridad en la consola de gestión.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en **Create Security Group**.
6. En el área **Create Security Group**, establezca los parámetros como se le solicite. **Tabla 2-3** enumera los parámetros que se van a configurar.

Figura 2-3 Crear Grupo de seguridad

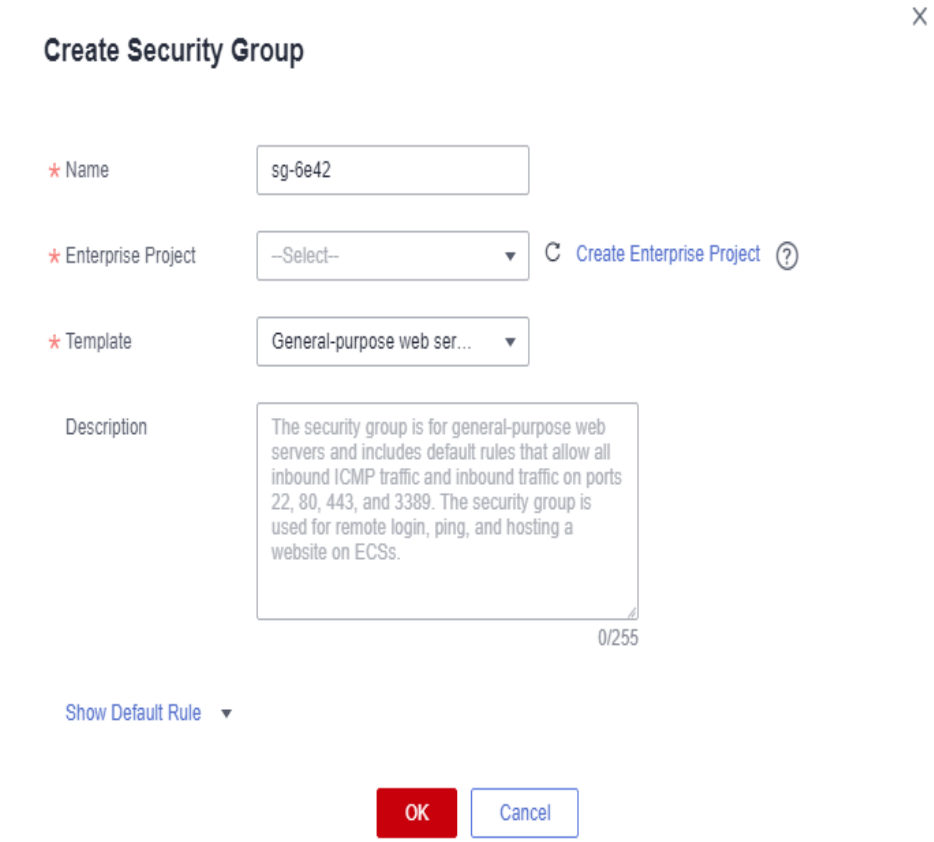


Tabla 2-3 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Plantilla	Una plantilla viene con reglas de grupo de seguridad predeterminadas, lo que le ayuda a crear rápidamente grupos de seguridad. Se proporcionan las siguientes plantillas: ● **Custom**: Esta plantilla le permite crear grupos de seguridad con reglas de grupo de seguridad personalizadas. ● **General-purpose web server**: el grupo de seguridad que se crea con esta plantilla es para servidores web de propósito general e incluye reglas predeterminadas que permiten todo el tráfico ICMP entrante y el tráfico entrante en los puertos 22, 80, 443 y 3389. ● **All ports open**: el grupo de seguridad que cree con esta plantilla incluye reglas predeterminadas que permiten el tráfico entrante en cualquier puerto. Tenga en cuenta que permitir el tráfico entrante en cualquier puerto plantea riesgos de seguridad.	Servidor web de uso general
Name	Nombre del grupo de seguridad. Este parámetro es obligatorio. El nombre del grupo de seguridad puede contener un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios. **NOTA** Puede cambiar el nombre del grupo de seguridad después de crear un grupo de seguridad. Se recomienda que asigne a cada grupo de seguridad un nombre diferente.	sg-318b
Enterprise Project	Al crear un grupo de seguridad, puede agregar el grupo de seguridad a un proyecto de empresa habilitado. Un proyecto empresarial facilita la gestión a nivel de proyectos y el agrupamiento de los recursos y usuarios en la nube. El nombre del proyecto predeterminado es **default**.	default
Description	Información adicional sobre el grupo de seguridad. Este parámetro es opcional. La descripción del grupo de seguridad puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. Haga clic en **OK**.

Operaciones relacionadas

- Para cada grupo de seguridad, puede agregar reglas que controlen el tráfico entrante a los ECS y un conjunto separado de reglas que controlen el tráfico saliente. Para más detalles, consulte **Adición de una regla de grupo de seguridad**.
- Cada ECS debe estar asociado con al menos un grupo de seguridad. Puede agregar un ECS a varios grupos de seguridad según los requisitos de servicio. Para más detalles, consulte **Adición y eliminación de instancias de un grupo de seguridad**.

2.1.5 Adición de una regla de grupo de seguridad

Escenarios

Un grupo de seguridad es una colección de reglas de control de acceso para recursos en la nube, como servidores en la nube, contenedores y bases de datos, para controlar el tráfico entrante y saliente. Los recursos de la nube asociados con el mismo grupo de seguridad tienen los mismos requisitos de seguridad y son de confianza mutua dentro de una VPC.

Si las reglas del grupo de seguridad asociado a la instancia no pueden cumplir sus requisitos, por ejemplo, debe permitir el tráfico entrante en un puerto de TCP especificado, puede agregar una regla entrante.

- Las reglas entrantes controlan el tráfico entrante a los recursos de la nube en el grupo de seguridad.
- Las reglas salientes controlan el tráfico saliente de los recursos de la nube en el grupo de seguridad.

Para obtener más información sobre las reglas de grupo de seguridad predeterminadas, consulte **Grupos de seguridad predeterminados y reglas de grupos de seguridad**. Para obtener más información acerca de los ejemplos de configuración de reglas de grupo de seguridad, consulte **Ejemplos de configuración de grupo de seguridad**.

Prerrequisitos

- Se ha creado un grupo de seguridad. Para obtener más información sobre cómo crear un grupo de seguridad, consulte **Creación de un grupo de seguridad**.
- Ha planificado las redes públicas o las privadas que pueden o no pueden acceder a instancias, como los ECS. Para obtener más ejemplos de reglas de grupo de seguridad, consulte **Ejemplos de configuración de grupo de seguridad**.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, busque el grupo de seguridad de destino y haga clic en **Manage Rule** en la columna **Operation** para cambiar a la página de gestión de reglas entrantes y salientes.

6. En la ficha **Inbound Rules**, haga clic en **Add Rule**. En el cuadro de diálogo que se muestra, establezca los parámetros necesarios para agregar una regla entrante.

   Puede hacer clic en + para agregar más reglas entrantes.

Figura 2-4 Agregar regla de entrada

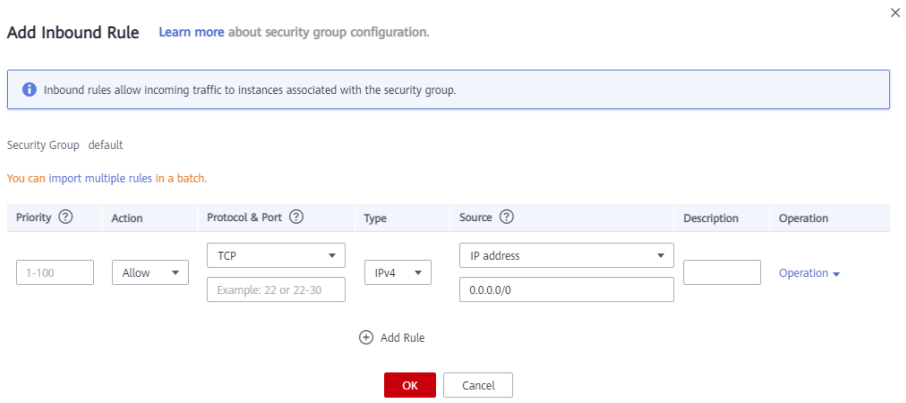


Tabla 2-4 Descripción del parámetro de regla entrante

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad oscila entre 1 y 100. El valor por defecto es 1 e indica la prioridad principal. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Las acciones de la regla del grupo de seguridad. Las reglas de denegación tienen prioridad sobre las reglas de permiso de la misma prioridad.	Allow
Protocol & Port	**Protocol**: El protocolo de red. Actualmente, el valor puede ser **All**, **TCP**, **UDP**, **ICMP**, **GRE** u otros.	TCP
	Port: El puerto o rango de puertos sobre el cual el tráfico puede llegar a su ECS. El valor oscila entre 1 y 65535. Ingrese los puertos en el siguiente formato: ● Puerto individual: Ingrese un puerto, como 22. ● Puertos consecutivos: Ingrese un rango de puertos, como 22-30. ● Puertos no consecutivos: Ingrese los puertos y rangos de puertos, como **22,23-30**. Puede introducir un máximo de 20 puertos y rangos de puertos. Cada rango de puertos debe ser único. ● All ports: Leave it empty or enter 1-65535.	22, or 22-30

Parámetro	Descripción	Valor de ejemplo
Type	El tipo de dirección IP. Este parámetro sólo está disponible después de activar la función IPv6. ● IPv4 ● IPv6	IPv4
Source	El origen de la regla de grupo de seguridad. El valor puede ser una única dirección IP, un grupo de direcciones IP o un grupo de seguridad para permitir el acceso desde direcciones IP o instancias en el grupo de seguridad. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de seguridad: sg-abc ● Grupo de direcciones IP: ipGroup-test Si el origen es un grupo de seguridad, esta regla se aplicará a todas las instancias asociadas con el grupo de seguridad seleccionado.	0.0.0.0/0
Description	Información complementaria sobre la regla del grupo de seguridad. Este parámetro es opcional. La descripción de la regla del grupo de seguridad puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. En la ficha **Outbound Rules**, haga clic en **Add Rule**. En el cuadro de diálogo que se muestra, establezca los parámetros necesarios para agregar una regla saliente.

   Puede hacer clic en + para agregar más reglas salientes.

Figura 2-5 Agregar regla de salida

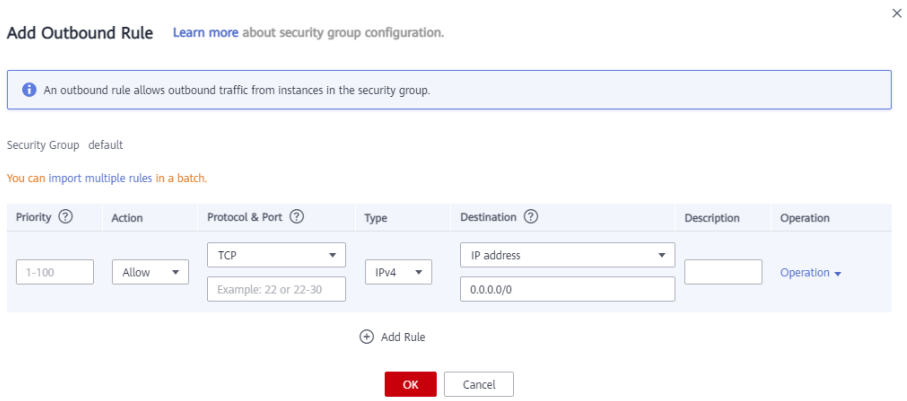


Tabla 2-5 Descripción del parámetro de regla saliente

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad oscila entre 1 y 100. El valor por defecto es 1 e indica la prioridad principal. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Las acciones de la regla del grupo de seguridad. ● **Allow**: permite el tráfico saliente de instancias del grupo de seguridad basado en la regla. ● **Deny**: deniega el tráfico saliente de las instancias del grupo de seguridad según la regla. Las reglas de denegación tienen prioridad sobre las reglas de permiso de la misma prioridad.	Allow
Protocol & Port	**Protocol**: El protocolo de red. Actualmente, el valor puede ser **All**, **TCP**, **UDP**, **ICMP**, **GRE** u otros.	TCP
	Port: El puerto o rango de puertos sobre el que el tráfico puede salir de su ECS. El valor oscila entre 1 y 65535.	22, or 22-30
Type	El tipo de dirección IP. ● IPv4 ● IPv6	IPv4
Destination	Destino de la regla de grupo de seguridad. El valor puede ser una única dirección IP, un grupo de direcciones IP o un grupo de seguridad para permitir el acceso a direcciones IP o instancias en el grupo de seguridad. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de seguridad: sg-abc ● Grupo de direcciones IP: ipGroup-test	0.0.0.0/0
Description	Información complementaria sobre la regla del grupo de seguridad. Este parámetro es opcional. La descripción de la regla del grupo de seguridad puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

8. Haga clic en **OK**.

Verificación

Después de agregar las reglas de grupo de seguridad necesarias, puede verificar que las reglas surtan efecto. 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 2-6**.

Tabla 2-6 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:

1. Inicie sesión en el ECS.
2. 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 2-6**, se está escuchando el puerto TCP 80.

   Figura 2-6 Salida del comando para ECS de Linux

3. 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:

1. Inicie sesión en el ECS.
2. Elija **Start** > **Accessories** > **Command Prompt**.
3. 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 2-7**, se está escuchando el puerto TCP 80.

   Figura 2-7 Salida del comando para Windows ECS

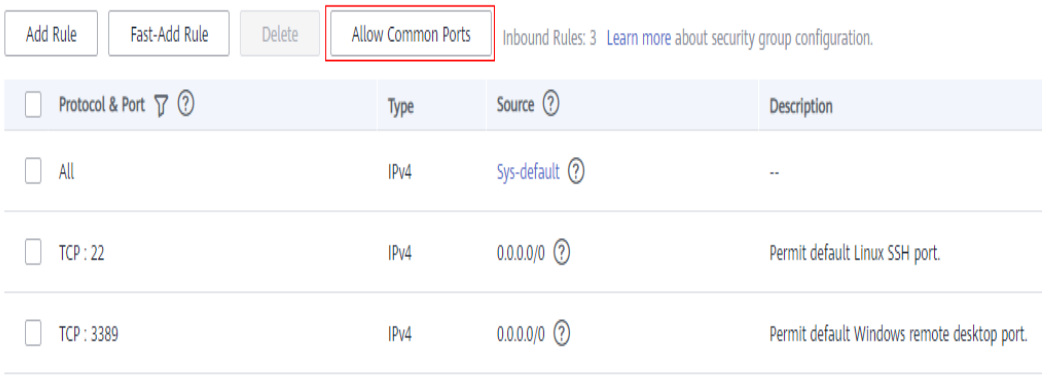
4. Escriba **http://***ECS EIP* en el cuadro de dirección del navegador y pulse **Enter**.
   Si se puede acceder a la página solicitada, la regla del grupo de seguridad tiene efecto.

Operaciones relacionadas

Allow Common Ports

Puede hacer clic en **Allow Common Ports** para permitir el tráfico en algunos puertos comunes, como los puertos 21, 22, 3389, 80, 443 y 20.

Figura 2-8 Permitir los puertos comunes



2.1.6 Reglas de grupo de seguridad de adición rápida

Escenarios

Puede agregar varias reglas de grupo de seguridad con diferentes protocolos y puertos al mismo tiempo.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, busque el grupo de seguridad de destino y haga clic en **Manage Rule** en la columna **Operation** para cambiar a la página de gestión de reglas entrantes y salientes.
6. En la ficha **Inbound Rules**, haga clic en **Fast-Add Rule**. En el cuadro de diálogo que aparece, seleccione los protocolos y puertos que desea agregar todos a la vez.

Figura 2-9 Regla de entrada de incorporación rápida

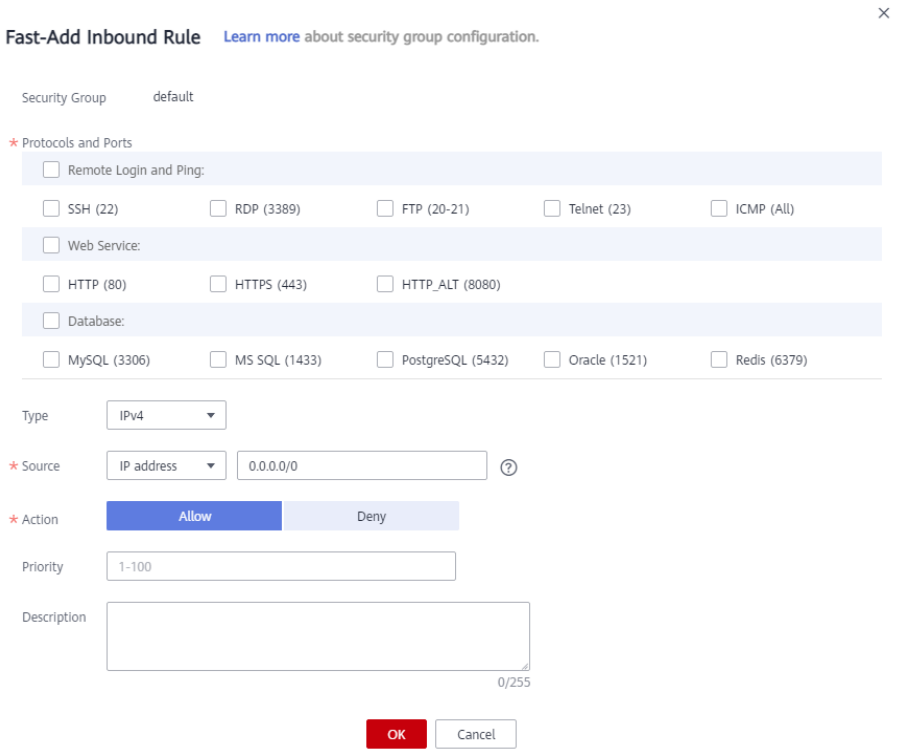


Tabla 2-7 Descripción del parámetro de regla entrante

Parámetro	Descripción	Valor de ejemplo
Protocols and Ports	Se proporcionan protocolos y puertos comunes para: ● Inicio de sesión remoto y ping ● Servicios web ● Bases de datos	SSH (22)
Type	Versión de la dirección IP. Este parámetro solo está disponible después de que la función IPv6 está habilitada. ● IPv4 ● IPv6	IPv4

Parámetro	Descripción	Valor de ejemplo
Source	Origen de la regla de grupo de seguridad. El valor puede ser una dirección IP, un grupo de direcciones IP o un grupo de seguridad para permitir el acceso desde direcciones IP o instancias en el grupo de seguridad. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de seguridad: sg-abc ● Grupo de direcciones IP: ipGroup-test Si el origen es un grupo de seguridad, esta regla se aplicará a todas las instancias asociadas con el grupo de seguridad seleccionado.	0.0.0.0/0
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad es de 1 a 100. El valor por defecto es 1 e indica la prioridad principal. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Acciones de regla de grupo de seguridad. Las reglas de denegación tienen prioridad sobre las reglas de permiso de la misma prioridad.	Allow
Description	(Opcional) Información complementaria sobre la regla del grupo de seguridad. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

7. En la ficha **Outbound Rules**, haga clic en **Fast-Add Rule**. En el cuadro de diálogo que se muestra, seleccione los protocolos y puertos necesarios para agregar varias reglas a la vez.

Figura 2-10 Regla de salida de incorporación rápida

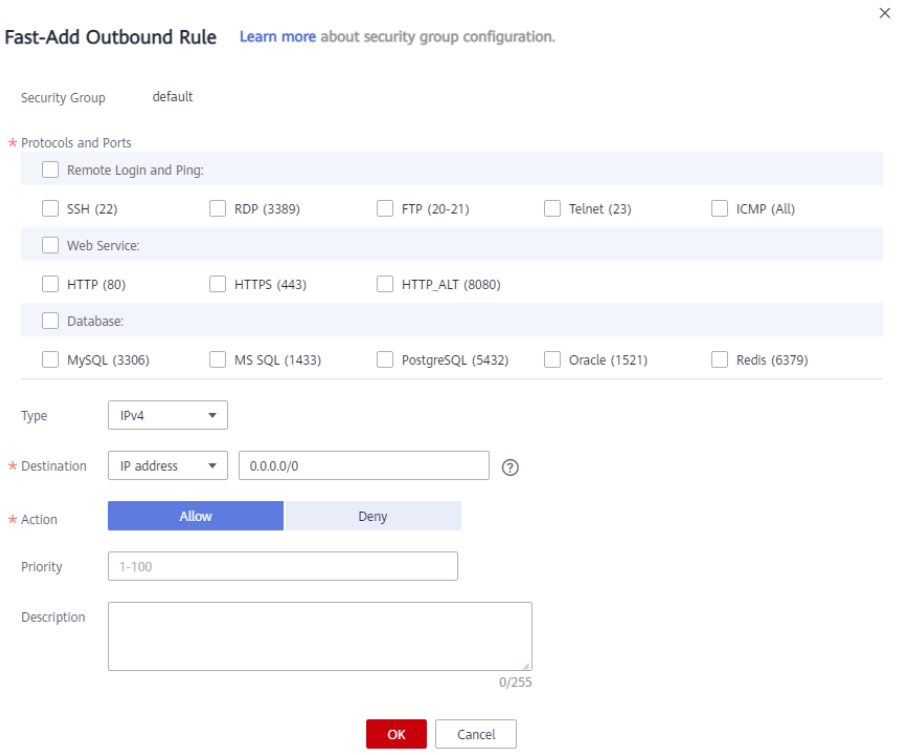


Tabla 2-8 Descripción del parámetro de regla saliente

Parámetro	Descripción	Valor de ejemplo
Protocols and Ports	Se proporcionan protocolos y puertos comunes para: ● Inicio de sesión remoto y ping ● Servicios web ● Bases de datos	SSH (22)
Type	Versión de la dirección IP. ● IPv4 ● IPv6	IPv4

Parámetro	Descripción	Valor de ejemplo
Destination	Destino de la regla de grupo de seguridad. El valor puede ser una dirección IP, un grupo de direcciones IP, o un grupo de seguridad para permitir el acceso a direcciones IP o instancias en el grupo de seguridad. Por ejemplo: ● xxx.xxx.xxx.xxx/32 (dirección IPv4) ● xxx.xxx.xxx.0/24 (rango de direcciones IPv4) ● 0.0.0.0/0 (todas las direcciones IPv4) ● sg-abc (grupo de seguridad) ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de seguridad: sg-abc ● Grupo de direcciones IP: ipGroup-test	0.0.0.0/0
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad es de 1 a 100. El valor por defecto es 1 e indica la prioridad principal. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Acciones de regla de grupo de seguridad. ● **Allow**: permite el tráfico saliente de instancias del grupo de seguridad basado en la regla. ● **Deny**: deniega el tráfico saliente de las instancias del grupo de seguridad según la regla. Las reglas de denegación tienen prioridad sobre las reglas de permiso de la misma prioridad.	Allow
Description	(Opcional) Información complementaria sobre la regla del grupo de seguridad. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

8. Haga clic en **OK**.

2.1.7 Replicación de una regla de grupo de seguridad

Escenarios

Replica una regla de grupo de seguridad existente para generar una nueva regla. Al replicar una regla de grupo de seguridad, puede realizar cambios para que no sea una copia perfecta.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en el nombre del grupo de seguridad.
6. En la página mostrada, busque la fila que contiene la regla de grupo de seguridad que se va a replicar y haga clic en **Replicate** en la columna **Operation**.

   También puede modificar la regla de grupo de seguridad según sea necesario para generar rápidamente una nueva regla.
7. Haga clic en **OK**.

2.1.8 Modificación de una regla de grupo de seguridad

Escenarios

Las reglas de grupo de seguridad inadecuadas pueden causar serios riesgos de seguridad. Por ejemplo, las reglas de grupo de seguridad permiten el acceso a puertos específicos. Puede modificar el puerto, el protocolo y la dirección IP de dichas reglas para garantizar la seguridad de sus instancias.

Prerrequisitos

Se ha creado un grupo de seguridad y se han agregado reglas de grupo de seguridad al grupo de seguridad.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en el nombre del grupo de seguridad.
6. En la página mostrada, busque la fila que contiene la regla de grupo de seguridad que se va a modificar y haga clic en **Modify** en la columna **Operation**.
7. Modifique la regla y haga clic en **Confirm**.

2.1.9 Eliminación de una regla de grupo de seguridad

Escenarios

Si es necesario cambiar el origen de una regla de grupo de seguridad entrante o el destino de una regla de grupo de seguridad saliente, primero debe eliminar la regla de grupo de seguridad y agregar una nueva.

NOTA

Las reglas de grupo de seguridad utilizan listas blancas. La eliminación de una regla de grupo de seguridad puede provocar errores de acceso de ECS.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en el nombre del grupo de seguridad.
6. Si no necesita una regla de grupo de seguridad, busque la fila que contiene la regla de destino y haga clic en **Delete**.
7. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Eliminar varias reglas de grupo de seguridad a la vez

También puede seleccionar varias reglas de grupo de seguridad y hacer clic en **Delete** encima de la lista de reglas de grupo de seguridad para eliminar varias reglas a la vez.

2.1.10 Importación y exportación de reglas de grupo de seguridad

Escenarios

- Si desea crear o restaurar rápidamente reglas de grupo de seguridad, puede importar reglas existentes al grupo de seguridad.
- Si desea realizar una copia de seguridad de las reglas del grupo de seguridad localmente, puede exportar las reglas a un archivo de Excel.
- Si desea aplicar rápidamente las reglas de un grupo de seguridad a otro, o si desea modificar varias reglas del grupo de seguridad actual a la vez, puede importar o exportar reglas existentes.

Notas y restricciones

- Al modificar las reglas del grupo de seguridad exportado, sólo puede modificar los campos existentes en el archivo exportado basándose en la plantilla y no puede agregar nuevos campos ni modificar los nombres de los campos. De lo contrario, el archivo no se importará.

- Al importar reglas de grupo de seguridad, si el origen es un grupo de direcciones IP, asegúrese de que el grupo de direcciones IP existe y que su nombre e ID son correctos. El formato es **ipGroup-zy[2b5213cb-0f41-4d0b-bed9-b6340bf51017]**.
- No se permiten las reglas duplicadas.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en el nombre del grupo de seguridad.
6. Exportar e importar las reglas de grupo de seguridad.
   - Haga clic en para exportar todas las reglas del grupo de seguridad actual a un archivo de Excel.
   - Haga clic en para importar reglas de grupo de seguridad desde un archivo de Excel al grupo de seguridad actual.

     Tabla 2-9 describe los parámetros de la plantilla para importar reglas.

     Tabla 2-9 Parámetros de plantilla

Parámetro	Descripción	Valor de ejemplo
Direction	Dirección en la que entra en vigor la regla de grupo de seguridad. ● Las reglas entrantes controlan el tráfico entrante a los recursos de la nube en el grupo de seguridad. ● Las reglas salientes controlan el tráfico saliente de los recursos de la nube en el grupo de seguridad.	Inbound
Priority	El valor de prioridad oscila entre 1 y 100. El valor por defecto es 1 e indica la prioridad principal. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Las reglas de denegación tienen prioridad sobre las reglas de permiso de la misma prioridad.	Allow
Protocol & Port	**Protocol**: El protocolo de red. Actualmente, el valor puede ser **All**, **TCP**, **UDP**, **ICMP**, **GRE** u otros.	TCP
	Port: El puerto o rango de puertos sobre el cual el tráfico puede llegar a su ECS. El valor oscila entre 1 y 65535.	22, or 22-30

Parámetro	Descripción	Valor de ejemplo
Type	El tipo de dirección IP. Este parámetro sólo está disponible después de activar la función IPv6. ● IPv4 ● IPv6	IPv4
Source	El origen de la regla de grupo de seguridad. El valor puede ser una única dirección IP, un grupo de direcciones IP o un grupo de seguridad para permitir el acceso desde direcciones IP o instancias en el grupo de seguridad. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de seguridad: sg-abc ● Grupo de direcciones IP: ipGroup-test	0.0.0.0/0
Destination	Destino de la regla de grupo de seguridad. El valor puede ser una única dirección IP, un grupo de direcciones IP o un grupo de seguridad para permitir el acceso a direcciones IP o instancias en el grupo de seguridad. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6) ● Grupo de seguridad: sg-abc ● Grupo de direcciones IP: ipGroup-test	0.0.0.0/0
Description	Información complementaria sobre la regla del grupo de seguridad. Este parámetro es opcional. La descripción de la regla del grupo de seguridad puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-
Last Modified	La hora en que se modificó el grupo de seguridad.	-

2.1.11 Eliminación de un grupo de seguridad

Escenarios

En esta sección se describe cómo eliminar grupos de seguridad que ya no son necesarios.

Notas y restricciones

- 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.

  Si no puede eliminar un grupo de seguridad incluso después de eliminar todas las instancias asociadas, **envíe un ticket de servicio**.

Prerrequisitos

- 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.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, busque la fila que contiene el grupo de seguridad de destino, haga clic en **More** en la columna **Operation** y haga clic en **Delete**.
6. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

2.1.12 Adición y eliminación de instancias de un grupo de seguridad

Escenarios

Después de crear un grupo de seguridad, puede agregar instancias al grupo de seguridad para proteger las instancias. También puede eliminarlos del grupo de seguridad según sea necesario.

Puede agregar varias instancias o eliminarlas de un grupo de seguridad.

Adición de instancias a un grupo de seguridad

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en **Manage Instance** en la columna **Operation**.
6. En la ficha **Servers**, haga clic en **Add** y agregue uno o más servidores al grupo de seguridad actual.
7. En la ficha **Extension NICs**, haga clic en **Add** y agregue una o más NIC de extensión al grupo de seguridad actual.
8. Haga clic en **OK**.

Eliminación de instancias de un grupo de seguridad

NOTA

- Se han agregado instancias a dos o más grupos de seguridad.
- Las instancias eliminadas de un grupo de seguridad no pueden comunicarse con otras instancias de este grupo de seguridad. Asegúrese de que sus instancias no se verán afectadas negativamente antes de eliminar instancias de un grupo de seguridad.

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en **Manage Instance** en la columna **Operation**.
6. En la ficha **Servers**, busque el servidor de destino y haga clic en **Remove** en la columna **Operation** para quitar el servidor del grupo de seguridad actual.
7. En la ficha **Extension NICs**, busque la extensión NIC de destino y haga clic en **Remove** en la columna **Operation** para quitar la NIC del grupo de seguridad actual.
8. Haga clic en **Yes**.

Eliminación de varias instancias de un grupo de seguridad

Seleccione varios servidores y haga clic en **Remove** encima de la lista de servidores para eliminar todos los servidores seleccionados del grupo de seguridad actual a la vez.

Seleccione varias NIC de extensión y haga clic en **Remove** encima de la lista de NIC de extensión para quitar todas las NIC de extensión seleccionadas del grupo de seguridad actual a la vez.

2.1.13 Clonación de un grupo de seguridad

Escenarios

Puede clonar un grupo de seguridad de una región a otra para aplicar rápidamente las reglas del grupo de seguridad a los ECS de otra región.

Puede clonar un grupo de seguridad en los siguientes escenarios:

- Por ejemplo, tiene el grupo de seguridad **sg-A** en la región A. Si los ECS de la región B requieren las mismas reglas de grupo de seguridad que las configuradas para el grupo de seguridad **sg-A**, puede clonar el grupo de seguridad **sg-A** en la región B, lo que le libera de crear un nuevo grupo de seguridad en la región B.
- Si necesita las nuevas reglas de grupo de seguridad, puede clonar el grupo de seguridad original como una copia de seguridad.

Notas y restricciones

Si clona un grupo de seguridad entre regiones, el sistema clonará sólo las reglas cuyo origen y destino sean bloques CIDR o estén en el grupo de seguridad actual.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, busque la fila que contiene el grupo de seguridad de destino y elija **More** > **Clone** en la columna **Operation**.
6. Defina los parámetros necesarios y haga clic en **OK**.

   A continuación, puede cambiar a la región necesaria para ver el grupo de seguridad clonado en la lista de grupos de seguridad.

2.1.14 Modificación de nombre de grupo de seguridad

Escenarios

Modifique el nombre y la descripción de un grupo de seguridad creado.

Procedimiento

Método 1

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.

4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, busque el grupo de seguridad de destino y elija **More** > **Modify** en la columna **Operation**.
6. Modifique el nombre y la descripción del grupo de seguridad según sea necesario.
7. Haga clic en **OK**.

Método 2

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **Security Groups**.
5. En la página **Security Groups**, haga clic en el nombre del grupo de seguridad.
6. En la página mostrada, haga clic en a la derecha de **Name** y edite el nombre del grupo de seguridad.
7. Haga clic en √ para guardar el nombre del grupo de seguridad.
8. Haga clic en a la derecha de **Description** y edite la descripción del grupo de seguridad.
9. Haga clic en √ para guardar la descripción del grupo de seguridad.

2.1.15 Consulta del grupo de seguridad de un ECS

Escenarios

Ver las reglas entrantes y salientes de un grupo de seguridad utilizado por un ECS.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En **Compute**, haga clic en **Elastic Cloud Server**.
4. En la página **Elastic Cloud Server**, haga clic en el nombre del ECS de destino.
5. Haga clic en la ficha **Security Groups** y vea información sobre el grupo de seguridad utilizado por el ECS.

2.1.16 Cambio del grupo de seguridad de un ECS

Escenarios

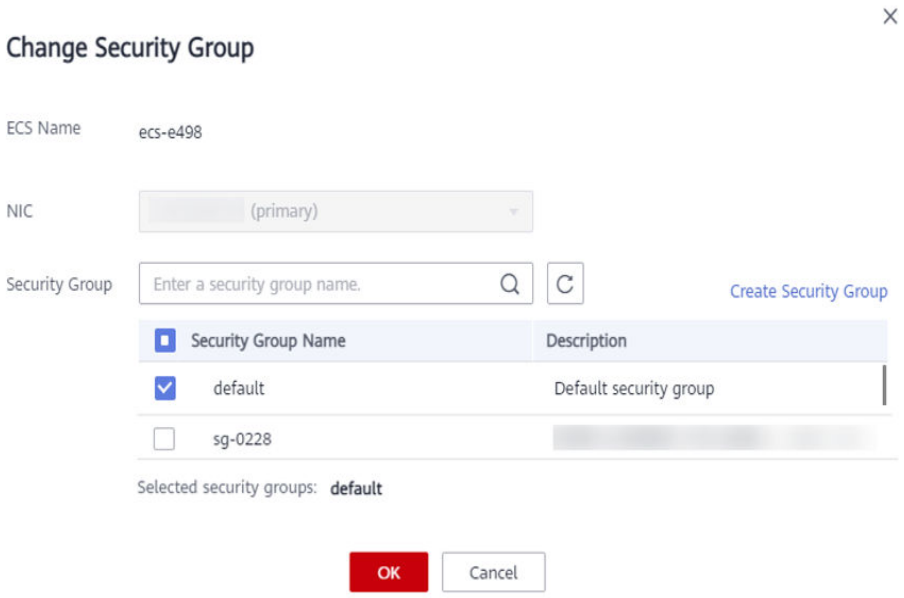
Cambie el grupo de seguridad asociado a una NIC de ECS.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en . En **Compute**, haga clic en **Elastic Cloud Server**.
3. En la lista ECS, busque la fila que contiene el ECS de destino. Haga clic en **More** en la columna **Operation** y seleccione **Manage Network** > **Change Security Group**.

   Aparece el cuadro de diálogo **Change Security Group**.

   Figura 2-11 Cambiar el grupo de seguridad



4. Seleccione la NIC de destino y los grupos de seguridad según se le solicite.

   Puede seleccionar varios grupos de seguridad. En tal caso, las reglas de todos los grupos de seguridad seleccionados se agregarán para aplicar en el ECS.

   Para crear un grupo de seguridad, haga clic en **Create Security Group**.

   NOTA

   El uso de varios grupos de seguridad puede deteriorar el rendimiento de la red de ECS. Se sugiere que seleccione no más de cinco grupos de seguridad.
5. Haz clic en **OK**.

2.1.17 Puertos comunes usados por los ECS

Al agregar una regla de grupo de seguridad, debe especificar el puerto o el rango de puertos para la comunicación. Cuando un grupo de seguridad detecta una solicitud de acceso, compruebe si las reglas de grupo de seguridad permiten la dirección IP y el puerto del dispositivo que envía la solicitud. La comunicación de datos solo se puede establecer cuando las reglas del grupo de seguridad permiten la solicitud.

Tabla 2-10 enumera los puertos comunes utilizados por los ECS. Puede configurar reglas de grupo de seguridad para permitir el tráfico hacia y desde los puertos ECS especificados. Para más detalles, consulte **Adición de una regla de grupo de seguridad**.

Tabla 2-10 Puertos comunes usados por los ECS

Protocolo	Puerto	Descripción
FTP	21	Utilizado para cargar y descargar archivos.
SSH	22	Utilizado para conectarse remotamente a los ECS Linux.
Telnet	23	Se utiliza para iniciar sesión de forma remota en ECS mediante Telnet
SMTP	25	Utilizado para enviar correos electrónicos Por motivos de seguridad, el puerto TCP 25 está deshabilitado por defecto en la dirección de salida.
HTTP	80	Se utiliza para acceder a sitios web sobre HTTP
POP3	110	Se utiliza para recibir correos electrónicos utilizando el protocolo de oficina postal versión 3 (POP3)
IMAP	143	Se utiliza para recibir los correos electrónicos mediante Internet Message Access Protocol (IMAP)
HTTPS	443	Utilizado para acceder sitios web sobre HTTPS
SQL Server	1433	Un puerto TCP de Microsoft SQL Server para la prestación de servicios
SQL Server	1434	Un puerto UDP de Microsoft SQL Server para devolver el número de puerto TCP/IP utilizado por SQL Server
Oracle	1521	Puerto de comunicaciones de la base de datos de Oracle, que debe estar habilitado en los ECS donde se despliega SQL Server de Oracle.
MySQL	3306	Utilizado por bases de datos MySQL para proporcionar servicios.
Windows Server Remote Desktop Services	3389	Se utiliza para conectarse a ECS de Windows
Proxy	8080	El puerto proxy 8080 utilizado en el servicio de proxy WWW para la navegación web. Si utiliza el puerto 8080, debe agregar **:8080** después de la dirección IP cuando visite un sitio web o use un servidor proxy. Una vez instalado Apache Tomcat, el puerto de servicio predeterminado es 8080.
NetBIOS	137, 138, and 139	NetBIOS se utiliza a menudo para archivos de Windows, uso compartido de impresoras y Samba. ● Puertos 137 y 138: puertos UDP que se utilizan al transferir archivos mediante Network Neighborhood (My Network Places) ● Puerto 139: Las conexiones desde este puerto intentan acceder al servicio NetBIOS/SMB.

Algunos puertos 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 2-11 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.

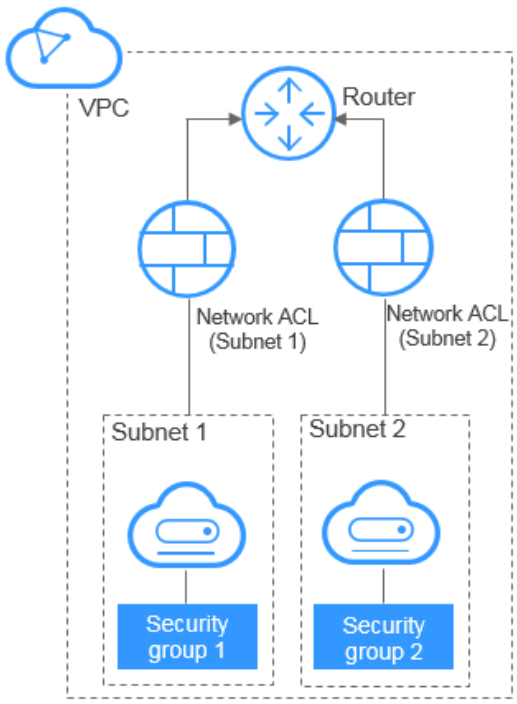
2.2 ACL de red

2.2.1 Descripción de ACL de red

Una ACL de red es una capa opcional de seguridad para sus subredes. Después de asociar una o más subredes a una ACL de red, puede controlar el tráfico de entrada y salida de las subredes.

Figura 2-12 muestra cómo funciona una ACL de red.shows how a firewall works.

Figura 2-12 Grupos de seguridad y ACL de red



Similar a los grupos de seguridad, las ACL de red controlan el acceso a las subredes y agregan una capa adicional de defensa a las subredes. Los grupos de seguridad solo tienen las reglas de "allow", pero las ACL de red tiene ambas reglas de "allow" y "deny". Puede utilizar las ACL de red junto con los grupos de seguridad para implementar un control de acceso completo y detallado. Puede utilizar las ACL de red junto con los grupos de seguridad para implementar un control de acceso completo y detallado.

Diferencias entre grupos de seguridad y ACL de red resume las diferencias básicas entre grupos de seguridad y ACL de red.

Conceptos básicos de la ACL de red

- Su VPC no viene con una ACL de red, pero puede crear una ACL de red y asociarla con una subred de VPC si es necesaria. De forma predeterminada, cada ACL de red deniega todo el tráfico entrante y saliente de la subred asociada hasta que agregue reglas.
- Puede asociar una ACL de red con varias subredes. Sin embargo, una subred solo se puede asociar a una ACL de red a la vez.
- Cada ACL de red recién creada se encuentra en el estado **Inactive** hasta que se asocien las subredes.
- Las ACL de red son de estado. Si envía una solicitud desde su instancia y se permite el tráfico saliente, se permite que el tráfico de respuesta para esa solicitud fluya independientemente de las reglas entrantes de ACL de red. De manera similar, si se permite el tráfico entrante, se permite que las respuestas al tráfico entrante permitido fluyan hacia fuera, independientemente de las reglas salientes.

  El periodo de tiempo de espera del seguimiento de la conexión varía según el protocolo. El periodo de tiempo de espera de una conexión TCP en el estado establecido es 600s, y el periodo de tiempo de espera de una conexión ICMP es 30s. Para otros protocolos, si se reciben paquetes en ambas direcciones, el periodo de tiempo de espera de seguimiento de conexión es de 180 segundos. Si se reciben uno o más paquetes en una dirección pero no se recibe ningún paquete en la otra dirección, el período de tiempo de espera de seguimiento de conexión es de 30 segundos. Para los protocolos distintos de TCP, UDP e ICMP, solo se realiza un seguimiento de la dirección IP y el número de protocolo.

Reglas por defecto de ACL de red

De forma predeterminada, cada ACL de red tiene reglas preestablecidas que permiten los siguientes paquetes:

- Paquetes cuyo origen y destino están en la misma subred
- Paquetes de difusión con el destino 255.255.255.255/32, que se utiliza para configurar la información de inicio del host.
- Paquetes de multidifusión con el destino 224.0.0.0/24, que es utilizado por los protocolos de enrutamiento.
- Paquetes de metadatos con el destino 169.254.169.254/32 y el puerto TCP número 80, que se utiliza para obtener metadatos.
- Paquetes de bloques CIDR reservados para servicios públicos (por ejemplo, paquetes con el destino 100.125.0.0/16)
- Una ACL de red niega todo el tráfico de entrada y salida de una subred, excepto los anteriores. **Tabla 2-12** muestra las reglas predeterminadas de ACL de red. No puede modificar ni eliminar las reglas predeterminadas.

Tabla 2-12 Reglas predeterminadas de ACL de red

Dirección	Prioridad	Acción	Protocolo	Fuente	Destino	Descripción
Entrante	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Deniega todo el tráfico entrante.
Saliente	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Deniega todo el tráfico saliente.

Prioridades de las reglas

- Cada regla de ACL de red tiene un valor de prioridad donde un valor más pequeño corresponde a una prioridad más alta. Cada vez que dos reglas entran en conflicto, la regla con la prioridad más alta es la que se aplica. La regla cuyo valor de prioridad es un asterisco (*) tiene la prioridad más baja.
- Si varias reglas de ACL de red entran en conflicto, solo la regla con la prioridad más alta tiene efecto. 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.

Escenarios de aplicación

- Si la capa de aplicación necesita proporcionar servicios a los usuarios, se debe permitir que el tráfico llegue a la capa de aplicación desde todas las direcciones IP. Sin embargo, también debe evitar el acceso ilegal de usuarios maliciosos.

  Solución: puede agregar reglas de ACL de red para denegar el acceso desde direcciones IP sospechosas.
- ¿Cómo puedo aislar puertos con vulnerabilidades identificadas? Por ejemplo, ¿cómo puedo aislar el puerto 445 que puede ser explotado por el gusano WannaCry?

  Solución: puede agregar reglas de ACL de red para denegar el tráfico de acceso desde un puerto y protocolo específicos, por ejemplo, el puerto TCP 445.
- No se requiere defensa para la comunicación dentro de una subred, pero se requiere control de acceso para la comunicación entre subredes.

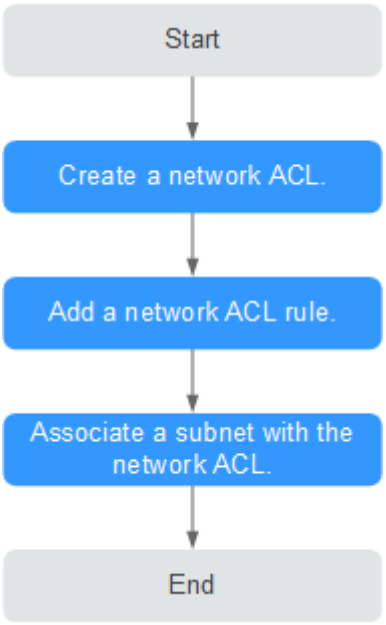
  Solución: puede agregar reglas de ACL de red para controlar el tráfico entre subredes.
- Para las aplicaciones a las que se accede con frecuencia, es posible que sea necesario ajustar una secuencia de reglas de seguridad para mejorar el rendimiento.

  Solución: Una ACL de red le permite ajustar la secuencia de reglas para que las reglas usadas con frecuencia se apliquen antes que otras reglas.

Proceso de configuración:

Figura 2-13 muestra el procedimiento para configurar una ACL de red.

Figura 2-13 Procedimiento de configuración de ACL de red



1. Cree una ACL de red siguiendo los pasos descritos en **Creación de una ACL de red**.
2. Agregue las reglas de ACL de red siguiendo los pasos descritos en **Adición de una regla de ACL de red**.
3. Asocie las subredes con la ACL de red siguiendo los pasos descritos en **Asociación de subredes con una ACL de red**. Después de asociar las subredes con la ACL de red, las subredes estarán protegidas por las reglas configuradas de ACL de red.

Restricciones de ACL de red

- De forma predeterminada, puede crear un máximo de 200 ACL de red en su cuenta en la nube.
- Puede asociar una ACL de red con varias subredes. Sin embargo, una subred solo se puede asociar a una ACL de red a la vez.
- Se recomienda que una ACL de red no contenga más de 20 reglas en una dirección. De lo contrario, su rendimiento puede deteriorarse.
- Para un rendimiento óptimo, no importa más de 40 reglas de ACL de red a la vez. Las reglas existentes seguirán estando disponibles después de importar las reglas nuevas. Cada regla se puede importar solo una vez.

2.2.2 Ejemplos de configuración de ACL de red

Esta sección proporciona ejemplos para configurar ACL de red.

- **Denegar el acceso desde un puerto específico**
- **Permitir el acceso desde puertos y protocolos específicos**
- **Denegar el acceso desde una dirección IP específica**

Denegar el acceso desde un puerto específico

Es posible que desee bloquear TCP 445 para protegerse contra los ataques de ransomware WannaCry. Puede agregar una regla de ACL de red para denegar todo el tráfico entrante desde el puerto TCP 445.

Configuraciones de ACL de red

Tabla 2-13 enumera la regla de entrada requerida.

Tabla 2-13 Reglas de ACL de red

Dirección	Acción	Protocolo	Fuente	Rango de puertos de origen	Destino	Rango de puertos de destino	Descripción
Entrante	Deny	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	445	Deniega el tráfico entrante de cualquier dirección IP a través del puerto TCP 445.
Entrante	Allow	All	0.0.0.0/0	1-65535	0.0.0.0/0	All	Permite todo el tráfico entrante.

NOTA

- De forma predeterminada, un ACL de red niega todo el tráfico entrante. Es necesario permitir todo el tráfico entrante si es necesario.
- Si desea que una regla de denegación coincida primero, inserte la regla de denegación encima de la regla de permiso. Para más detalles, consulte **Cambio de la secuencia de una regla de ACL de red**.

Permitir el acceso desde puertos y protocolos específicos

En este ejemplo, un ECS en una subred se utiliza como servidor web, y debe permitir el tráfico entrante desde el puerto HTTP 80 y el puerto HTTPS 443 y permitir todo el tráfico saliente. Es necesario configurar tanto las reglas de ACL de red como las reglas del grupo de seguridad para permitir el tráfico.

Configuraciones de ACL de red

Tabla 2-14 enumera la regla de entrada requerida.

Tabla 2-14 Reglas de ACL de red

Dirección	Acción	Protocolo	Fuente	Rango de puertos de origen	Destino	Rango de puertos de destino	Descripción
Entrante	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	80	Permite el tráfico HTTP entrante desde cualquier dirección IP a los ECS en la subred a través del puerto 80.
Entrante	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	443	Permite el tráfico HTTPS entrante desde cualquier dirección IP a los ECS en la subred a través del puerto 443.
Saliente	Allow	All	0.0.0.0/0	All	0.0.0.0/0	All	Permite todo el tráfico saliente de la subred.

Configuración del grupo de seguridad

Tabla 2-15 enumera las reglas de grupo de seguridad entrante y saliente requeridas.

Tabla 2-15 Reglas de grupos de seguridad

Dirección	Protocolo / Aplicación	Puerto	Origen/Destino	Descripción
Entrante	TCP	80	Origen: 0.0.0.0/0	Permite el tráfico HTTP entrante desde cualquier dirección IP a los ECS asociados con el grupo de seguridad a través del puerto 80.
Entrante	TCP	443	Origen: 0.0.0.0/0	Permite el tráfico HTTPS entrante desde cualquier dirección IP a los ECS asociados con el grupo de seguridad a través del puerto 443.

Dirección	Protocolo / Aplicación	Puerto	Origen/Destino	Descripción
Saliente	All	All	Destino: 0.0.0.0/0	Permite todo el tráfico saliente del grupo de seguridad.

Un ACL de red agrega una capa adicional de seguridad. Incluso si las reglas del grupo de seguridad permiten más tráfico del que realmente se requiere, las reglas de ACL de red solo permiten el acceso desde el puerto HTTP 80 y el puerto HTTPS 443 y niegan otro tráfico entrante.

Denegar el acceso desde una dirección IP específica

En este ejemplo, puede agregar una regla de ACL de red para denegar el acceso desde algunas direcciones IP anormales, por ejemplo, 192.168.1.102.

Configuraciones de ACL de red

Tabla 2-16 enumera las reglas de entrada requeridas.

Tabla 2-16 Reglas de ACL de red

Dirección	Acción	Protocolo	Fuente	Rango de puertos de origen	Destino	Rango de puertos de destino	Descripción
Entrante	Deny	TCP	192.168.1.102/32	1-65535	0.0.0.0/0	Todos	Deniega el acceso desde 192.168.1.102.
Entrante	Allow	All	0.0.0.0/0	1-65535	0.0.0.0/0	Todos	Permite todo el tráfico entrante.

NOTA

- De forma predeterminada, un ACL de red niega todo el tráfico entrante. Es necesario permitir todo el tráfico entrante si es necesario.
- Si desea que una regla de denegación coincida primero, inserte la regla de denegación encima de la regla de permiso. Para más detalles, consulte **Cambio de la secuencia de una regla de ACL de red**.

2.2.3 Creación de una ACL de red

Escenarios

Puede crear una ACL de red personalizada, pero cualquier ACL de red recién creada se desactivará por defecto. No tendrá ninguna regla entrante o saliente, ni tendrá ninguna subrede asociada. Cada usuario puede crear hasta 200 ACL de red por defecto.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. En el panel derecho que se muestra, haga clic en **Create ACL de red**.
6. En el cuadro de diálogo que se muestra, escriba la información de la ACL de red según se le solicite. **Tabla 2-17** enumera los parámetros que se van a configurar.

Figura 2-14 Crear la ACL de red

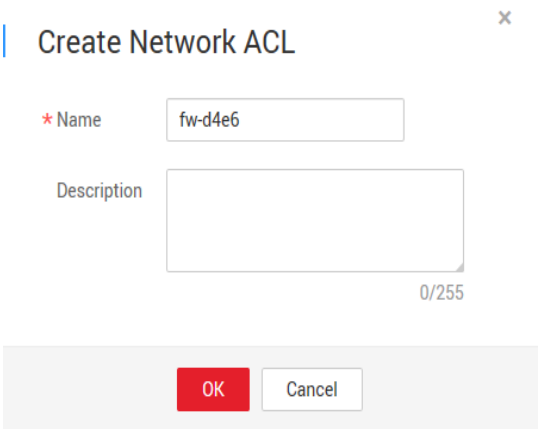


Tabla 2-17 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	El nombre de la ACL de red. Este parámetro es obligatorio. El nombre contiene un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_) y guiones (-). El nombre no puede contener espacios.	fw-92d3

Parámetro	Descripción	Valor de ejemplo
Description	Información complementaria sobre la ACL de red. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. Haga clic en **OK**.

2.2.4 Adición de una regla de ACL de red

Escenarios

Agregue una regla de entrada o de salida según los requisitos de seguridad de la red.

Se recomienda que una ACL de red no contenga más de 20 reglas en una dirección. De lo contrario, su rendimiento puede deteriorarse.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la ficha **Inbound Rules** o **Outbound Rules**, haga clic en **Add Rule** para agregar una regla de entrada o de salida.
   - Haga clic en + para agregar más reglas.
   - Busque la fila que contiene la regla de ACL de red y haga clic en **Replicate** en la columna **Operation** para replicar una regla existente.

   Tabla 2-18 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de la regla de ACL de red. Un valor de prioridad más pequeño indica una prioridad más alta. Cada ACL de red incluye una regla predeterminada cuyo valor de índice es un asterisco (*). Las reglas predeterminadas tienen la prioridad más baja.	3

Parámetro	Descripción	Valor de ejemplo
Status	Estado de una ACL de red. Cuando se agrega una regla, su estado predeterminado es **Enabled**.	Enabled
Type	Este parámetro sólo está disponible después de activar la función IPv6. El tipo de ACL de red. Este parámetro es obligatorio. Puede seleccionar un valor de la lista desplegable. Actualmente, solo se admiten IPv4 e IPv6.	IPv4
Action	La acción en la ACL de red. Este parámetro es obligatorio. Puede seleccionar un valor de la lista desplegable. Actualmente, el valor puede ser **Allow** o **Deny**.	Allow
Protocol	El protocolo soportado por la ACL de red. Este parámetro es obligatorio. Puede seleccionar un valor de la lista desplegable. El valor puede ser **TCP**, **UDP**, **All**, o **ICMP**. Si se selecciona **ICMP** o **All**, no es necesario especificar la información de puerto.	TCP
Source	El origen desde el que se permite el tráfico. El origen puede ser una dirección IP, un grupo de direcciones IP o un intervalo de direcciones IP. El valor predeterminado es 0.0.0.0/0, que indica que se permite el tráfico de todas las direcciones IP. Tanto el origen como el destino pueden utilizar el grupo de direcciones IP. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0
Source Port Range	El número de puerto de origen o el intervalo de número de puerto. El valor oscila entre 1 y 65535. Para un rango de número de puerto, introduzca dos números de puerto conectados por un guion (-). Por ejemplo, **1-100**. Debe especificar este parámetro si se selecciona TCP o UDP para **Protocol**.	22, o 22-30

Parámetro	Descripción	Valor de ejemplo
Destination	El destino al que se permite el tráfico. El origen puede ser una dirección IP, un grupo de direcciones IP o un intervalo de direcciones IP. El valor predeterminado es 0.0.0.0/0, que indica que se permite el tráfico a todas las direcciones IP. Tanto el origen como el destino pueden utilizar el grupo de direcciones IP. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0
Destination Port Range	El número de puerto de destino o el intervalo de número de puerto. El valor oscila entre 1 y 65535. Para un rango de número de puerto, introduzca dos números de puerto conectados por un guion (-). Por ejemplo, **1-100**. Debe especificar este parámetro si se selecciona TCP o UDP para **Protocol**.	22, or 22-30
Description	Información complementaria sobre la regla de la ACL de red. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. Haga clic en **OK**.

2.2.5 Asociación de subredes con una ACL de red

Escenarios

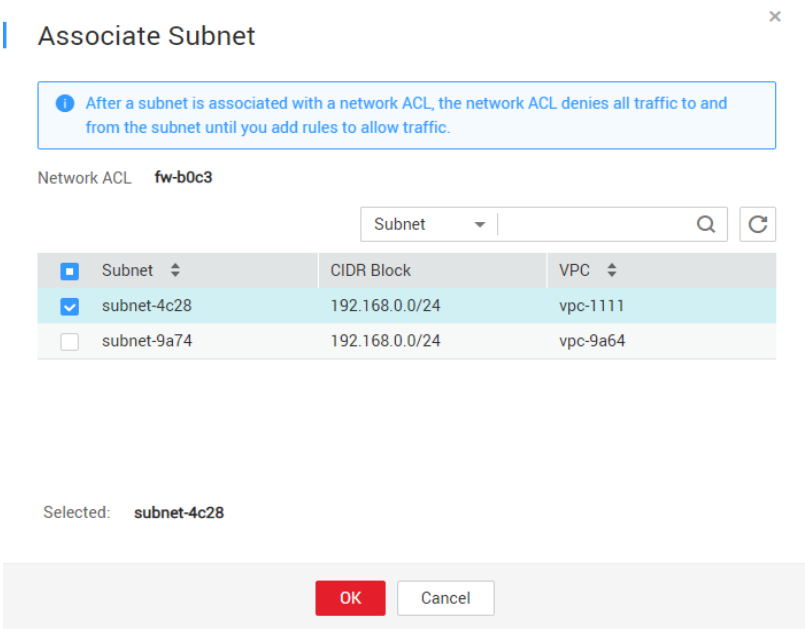
En la página que muestra los detalles en ACL de red, asocie las subredes deseadas con una ACL de red. Después de asociar una ACL de red con una subred, la ACL de red niega todo el tráfico hacia y desde la subred hasta que se agregan reglas para permitir el tráfico.

Procedimiento

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

3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la página mostrada, haga clic en la ficha **Associated Subnets**.
7. En la página **Associated Subnets**, haga clic en **Associate**.

Figura 2-15 Asociar subred



8. En la página mostrada, seleccione las subredes que desea asociar con ACL de red y haga clic en **OK**.

NOTA

Las subredes que ya han sido asociadas a las ACL de red no se mostrarán en la página para que usted las seleccione. Actualmente no se admite la asociación y disociación de subred con un solo clic. Además, una subred solo puede asociarse con una ACL de red. Si desea volver a asociar una subred que ya ha sido asociada a otra ACL de red, primero debe disociar la subred de la ACL de red original.

2.2.6 Disociación de una subred de un ACL de red

Escenarios

Disocie una subred de una ACL de red cuando sea necesaria.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.

4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la página mostrada, haga clic en la ficha **Associated Subnets**.
7. En la página **Associated Subnets**, busque la fila que contiene la subred de destino y haga clic en **Disassociate** en la columna **Operation**.
8. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Disociación de subredes de una ACL de red

Seleccione varias subredes y haga clic en **Disassociate** encima de la lista de subred para disociar las subredes de la ACL de red actual a la vez.

2.2.7 Cambio de la secuencia de una regla de ACL de red

Escenarios

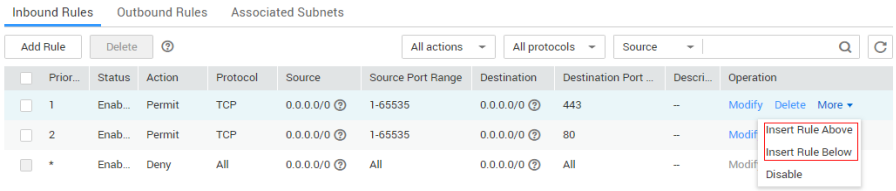
Si necesita que una regla surta efecto antes o después de una regla específica, puede insertar esa regla antes o después de la regla específica.

Si varias reglas de ACL de red entran en conflicto, solo la regla con la prioridad más alta tiene efecto.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la ficha **Inbound Rules** o **Outbound Rules**, busque la regla de destino, haga clic en **More** en la columna **Operation** y seleccione **Insert Rule Above** o **Insert Rule Below**.

Figura 2-16 Insertar una regla



7. En el cuadro de diálogo que aparece, configure los parámetros necesarios y haga clic en **OK**.

   Se inserta la regla. El procedimiento para insertar una regla saliente es el mismo que para insertar una regla entrante.

2.2.8 Modificación de una regla de ACL de red

Escenarios

Modifique una regla entrante o saliente de la ACL de red según los requisitos de seguridad de la red.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la ficha **Inbound Rules** o **Outbound Rules**, busque la fila que contiene la regla de destino y haga clic en **Modify** en la columna **Operation**. En el cuadro de diálogo que se muestra, configure los parámetros según se le solicite. **Tabla 2-19** enumera los parámetros que se van a configurar.

Tabla 2-19 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de la regla de ACL de red. Un valor de prioridad más pequeño indica una prioridad más alta. Cada ACL de red incluye una regla predeterminada cuyo valor de índice es un asterisco (*). Las reglas predeterminadas tienen la prioridad más baja.	3
Status	Estado de una ACL de red. Cuando se agrega una regla, su estado predeterminado es **Enabled**.	Enabled
Type	Este parámetro sólo está disponible después de activar la función IPv6. El tipo de ACL de red. Este parámetro es obligatorio. Puede seleccionar un valor de la lista desplegable. Actualmente, solo se admiten IPv4 e IPv6.	IPv4
Action	La acción en la ACL de red. Este parámetro es obligatorio. Puede seleccionar un valor de la lista desplegable. Actualmente, el valor puede ser **Allow** o **Deny**.	Allow

Parámetro	Descripción	Valor de ejemplo
Protocol	El protocolo soportado por la ACL de red. Este parámetro es obligatorio. Puede seleccionar un valor de la lista desplegable. El valor puede ser **TCP**, **UDP**, **All**, o **ICMP**. Si se selecciona **ICMP** o **All**, no es necesario especificar la información de puerto.	TCP
Source	El origen desde el que se permite el tráfico. El origen puede ser una dirección IP, un grupo de direcciones IP o un intervalo de direcciones IP. El valor predeterminado es 0.0.0.0/0, que indica que se permite el tráfico de todas las direcciones IP. Tanto el origen como el destino pueden utilizar el grupo de direcciones IP. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0
Source Port Range	El número de puerto de origen o el intervalo de número de puerto. El valor oscila entre 1 y 65535. Para un rango de número de puerto, introduzca dos números de puerto conectados por un guion (-). Por ejemplo, **1-100**. Debe especificar este parámetro si se selecciona TCP o UDP para **Protocol**.	22, o 22-30
Destination	El destino al que se permite el tráfico. El origen puede ser una dirección IP, un grupo de direcciones IP o un intervalo de direcciones IP. El valor predeterminado es 0.0.0.0/0, que indica que se permite el tráfico a todas las direcciones IP. Tanto el origen como el destino pueden utilizar el grupo de direcciones IP. Por ejemplo: ● Dirección IP única: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) ● Intervalo de direcciones IP: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) ● Todas las direcciones IP: 0.0.0.0/0 (IPv4); ::/0 (IPv6)	0.0.0.0/0

Parámetro	Descripción	Valor de ejemplo
Destination Port Range	El número de puerto de destino o el intervalo de número de puerto. El valor oscila entre 1 y 65535. Para un rango de número de puerto, introduzca dos números de puerto conectados por un guion (-). Por ejemplo, **1-100**. Debe especificar este parámetro si se selecciona TCP o UDP para **Protocol**.	22, or 22-30
Description	Información complementaria sobre la regla de la ACL de red. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. Haga clic en **Confirm**.

2.2.9 Activación o desactivación de una regla de ACL de red

Escenarios

Habilitar o deshabilitar una regla de entrada o salida según los requisitos de seguridad de la red.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la ficha **Inbound Rules** o **Outbound Rules**, busque la fila que contiene la regla de destino y haga clic en **More** y, a continuación, en **Enable** o **Disable** en la columna **Operation**.
7. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

   La regla está activada o desactivada. El procedimiento para habilitar o deshabilitar una regla saliente es el mismo que para habilitar o deshabilitar una regla entrante.

2.2.10 Eliminación de una regla de ACL de red

Escenarios

Eliminar una regla de entrada o de salida según los requisitos de seguridad de la red.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la ficha **Inbound Rules** o **Outbound Rules**, busque la fila que contiene la regla de destino y haga clic en **Delete** en la columna **Operation**.
7. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Eliminar varias reglas deACL de red a la vez

También puede seleccionar varias reglas de ACL de red y hacer clic en **Delete** encima de la lista de reglas de ACL de red para eliminar varias reglas a la vez.

2.2.11 Exportación e importación de reglas de ACL de red

Escenarios

Puede exportar las reglas entrantes y salientes de una ACL de red específica como un archivo de Excel y luego importar estas reglas para otra ACL de red. Se admiten las reglas de importación y exportación entre las regiones.

Se recomienda que no importe más de 40 reglas cada vez. La importación de reglas no eliminará las reglas existentes. No se permiten las reglas duplicadas.

Exportación de reglas de ACL de red

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. Haga clic en para exportar las reglas entrantes y salientes de la ACL de red. Las reglas exportadas se almacenan en un archivo de Excel. Necesita descargar el archivo a un directorio local.

Importación de reglas de ACL de red

1. Inicie sesión en la consola de gestión.

2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. Para hacer clic en  :
7. Seleccione el archivo de Excel que contiene las reglas exportadas de ACL de red y haga clic en **Import** para importar las reglas.

2.2.12 Consulta de una ACL de red

Escenarios

Consultar detalles sobre una ACL de red.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la página que se muestra, haga clic en **Inbound Rules**, **Outbound Rules**, y **Associated Subnets** una por una para ver detalles sobre las reglas de entrada, las reglas de salida y las asociaciones de subredes.

2.2.13 Modificación de una ACL de red

Escenarios

Modifique el nombre y la descripción de una ACL de red.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.

5. Localice la ACL de red de destino y haga clic en su nombre para cambiar a la página que muestra los detalles de esa ACL de red particular.
6. En la página mostrada, haga clic en a la derecha de **Name** y edite el nombre de la ACL de red.
7. Haga clic para guardar el nuevo nombre de la ACL de red.
8. Haga clic en a la derecha de Description y edite la descripción de la ACL de red.
9. Haga clic para guardar la nueva descripción de la ACL de red.

2.2.14 Activación o desactivación de una ACL de red

Escenarios

Después de crear una ACL de red, es posible que deba habilitarla en función de los requisitos de seguridad de la red. También puede desactivar una ACL de red habilitado si es necesario. Antes de habilitar una ACL de red, asegúrese de que las subredes se han asociado con la ACL de red y que se han agregado reglas entrantes y salientes a la ACL de red.

Cuando una ACL de red está deshabilitada, las reglas personalizadas no serán válidas mientras las reglas predeterminadas sigan surtiendo efecto. Deshabilitar una ACL de red puede interrumpir el tráfico de red. Para obtener información sobre las reglas predeterminadas de ACL de red, consulte **Reglas por defecto de ACL de red**.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Busque la fila que contiene la ACL de red de destino en el panel derecho, haga clic en **More** en la columna **Operation** y haga clic en **Enable** o **Disable**.
6. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

2.2.15 Supresión de una ACL de red

Escenarios

Eliminar una ACL de red cuando ya no sea necesaria.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.

4. En el panel de navegación de la izquierda, elija **Access Control** > ACL de red.
5. Busque la ACL de red de destino en el panel derecho, haga clic en **More** en la columna **Operation** y haga clic en **Delete**.
6. Haga clic en **Yes**.

NOTA

Después de eliminar una ACL de red, las subredes asociadas se disocian y las reglas agregadas se eliminan de la ACL de red.

2.3 Diferencias entre grupos de seguridad y ACL de red

Puede configurar grupos de seguridad y ACL de red para aumentar la seguridad de los ECS en su VPC.

- Los grupos de seguridad operan a nivel de ECS.
- Se operan las ACL de red a nivel de subred.

Para más detalles, consulte **Figura 2-17**.

Figura 2-17 Grupos de seguridad y ACL de red

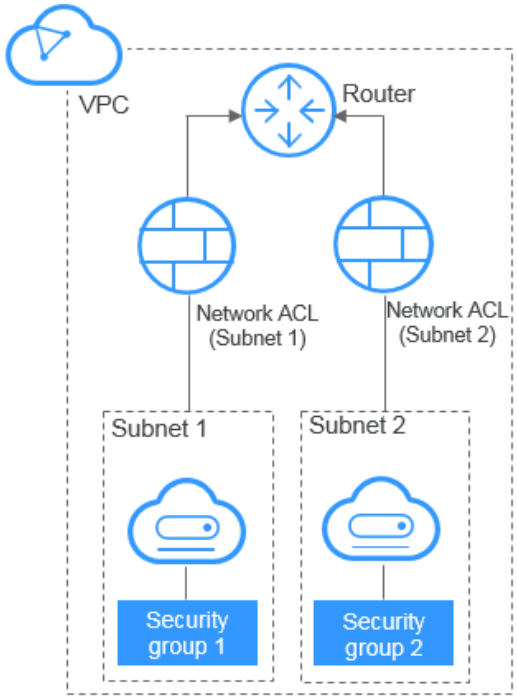


Tabla 2-20 describe las diferencias entre los grupos de seguridad y las ACL de red.

Tabla 2-20 Diferencias entre grupos de seguridad y ACL de red

Categoría	Grupo de seguridad	ACL de red
Objetivos	Funciona a nivel de ECS.	Funciona a nivel de subred.

Categoría	Grupo de seguridad	ACL de red
Reglas	Admite las reglas **Allow** y **Deny**. Las reglas de denegación solo se admiten en algunas regiones.	Admite las reglas **Allow** y **Deny**.
Prioridad	Si hay reglas en conflicto, las reglas tienen efecto en función de la secuencia de su grupo de seguridad al asociarse con un recurso y, a continuación, en función de las prioridades de regla en el grupo.	If rules conflict, the rule with the highest priority takes effect.
Usage	Se aplica automáticamente a los ECS del grupo de seguridad seleccionado durante la creación de ECS. Debe seleccionar un grupo de seguridad al crear ECS.	Se aplica a todos los ECS de las subredes asociadas al ACL de red. No se permite seleccionar una ACL de red durante la creación de la subred. Debe crear una ACL de red, asociar subredes con él, agregar reglas entrantes y salientes y habilitar la ACL de red. La ACL de red luego tiene efecto para las subredes asociadas y los ECS en las subredes.
Paquetes	Solo se admite el filtrado de paquetes basado en la 3-tupla (protocolo, puerto y dirección IP del par).	Sólo filtrado de paquetes basado en la 5-tupla (protocolo, puerto de origen, puerto de destino, dirección IP de origen y dirección IP de destino) es compatible.

2.4 Grupo de direcciones IP

2.4.1 Descripción general del grupo de direcciones IP

Un grupo de direcciones IP es una colección de direcciones IP que pueden usar la misma regla del grupo de seguridad. Un grupo de direcciones IP puede ser utilizado para gestionar direcciones IP que tengan los mismos requerimientos de seguridad o cuyos requerimientos de seguridad cambien de manera frecuente.

Puede crear un grupo de direcciones IP y agregar direcciones IP que deben gestionarse de manera unificada al grupo. A continuación, puede seleccionar este grupo de direcciones IP al configurar una regla del grupo de seguridad. La regla entrará en vigor para todas las direcciones IP del grupo de direcciones IP.

2.4.2 Creación de un grupo de direcciones IP

Escenarios

Cree un grupo de direcciones IP y agregue direcciones IP que deben gestionarse de forma centralizada a este grupo.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **IP Address Groups**.
5. Haga clic en **Create IP Address Group**.
6. Configure los parámetros requeridos. **Tabla 2-21** muestra los parámetros del grupo de direcciones IP.

Tabla 2-21 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	El nombre del grupo de direcciones IP. Este parámetro es obligatorio. El nombre del grupo de direcciones IP contiene un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios. Puede personalizar el nombre de un grupo de direcciones IP que se identifica de forma única por su ID.	ipGroup-f7de
IP Address Version	Obligatorio Actualmente, se admiten las siguientes versiones de direcciones IP: ● IPv4 ● IPv6	IPv4

Parámetro	Descripción	Valor de ejemplo
IP Address	Introduzca los intervalos de direcciones o las direcciones de IPv4 o de IPv6. Puede agregar un máximo de 20 direcciones IP o intervalos de direcciones IP, y cada una debe estar en una línea separada. Formatos admitidos: ● IPv4 – Rango de direcciones IP: Por ejemplo, 192.168.0.0/16 – Las direcciones IP consecutivas separaron un guion (-): Por ejemplo, 192.168.1.1-192.168.1.50 – Dirección IP única: Por ejemplo, 192.168.10.10 ● IPv6 – Intervalo de direcciones IPv6: Por ejemplo, 2001:db8:a583:6e::/64 – Direcciones IPv6 consecutivas separadas por un guion (-): Por ejemplo, 2001:db8:a583:6e::1-2001:db8:a583:6e::50 – Dirección IPv6 única: Por ejemplo, 2001:db8:a583:6e::5c	192.168.0.0/16 192.168.1.1-192.168.1.50 192.168.10.10
Description	Información adicional sobre el grupo de direcciones IP. Este parámetro es opcional. La descripción del grupo de direcciones IP puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. Haga clic en **OK**.

2.4.3 Asociación de un grupo de direcciones IP a una regla de grupo de seguridad

Escenarios

Seleccione un grupo de direcciones IP al agregar una regla del grupo de seguridad para que la regla se aplique a todas las direcciones IP del grupo de direcciones IP.

Procedimiento

Agregue una regla de grupo de seguridad haciendo referencia a **Adición de una regla de grupo de seguridad**. Preste atención a lo siguiente:

1. Seleccione **IP address group** de la lista desplegable para **Source**.
2. Seleccione el grupo de direcciones IP de destino.

Después de los pasos anteriores, el grupo de direcciones IP se puede asociar a la regla del grupo de seguridad.

2.4.4 Gestión de un grupo de direcciones IP

Escenarios

Modificar o eliminar un grupo de direcciones IP.

NOTA

- Después de modificar un grupo de direcciones IP, las direcciones de origen de sus reglas del grupo de seguridad asociadas también cambiarán.
- La eliminación de un grupo de direcciones IP también eliminará las reglas del grupo de seguridad asociadas con el grupo de direcciones IP.

Modificación de un grupo de direcciones IP

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **IP Address Groups**.
5. En la página mostrada, haga clic en **Modify** en la columna **Operación** para modificar el nombre, la dirección IP y la descripción del grupo de direcciones IP.

Eliminación de un grupo de direcciones IP

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Access Control** > **IP Address Groups**.
5. En la página **IP Address Groups**, busque el grupo de direcciones IP de destino y haga clic en **Delete** en la columna **Operation**. En la caja de diálogo que aparece, haga clic en **Yes**.

   La eliminación de un grupo de direcciones IP también eliminará las reglas de grupo de seguridad asociadas con el grupo de direcciones IP.

3 Elastic IP

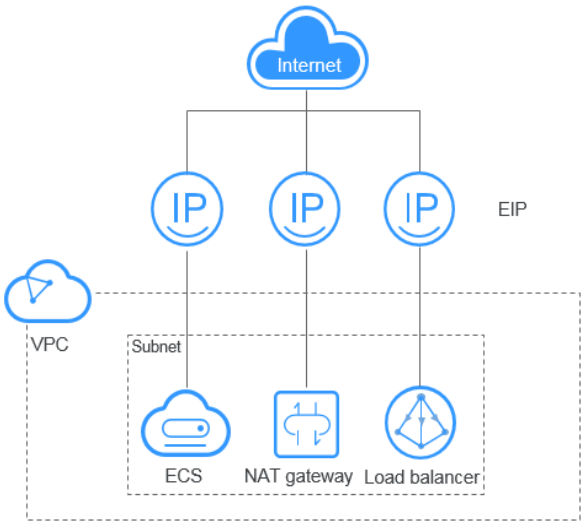
3.1 Descripción general de EIP

EIP

El servicio Elastic IP (EIP) le permite utilizar direcciones IP públicas estáticas y anchos de banda escalables para conectar sus recursos de nube a Internet. Los EIP pueden estar vinculados o independientes de ECS, BMS, direcciones IP virtuales, gateways NAT o balanceadores de carga. Se proporcionan varios modos de facturación para satisfacer diversos requisitos de servicio.

Cada EIP solo puede ser usado por un recurso en la nube a la vez.

Figura 3-1 Acceso a Internet con un EIP



Ventajas

- Flexibilidad

Un EIP puede asociarse de manera flexible con o disociarse del ECS, BMS, gateway NAT, equilibrador de carga o dirección IP virtual. El ancho de banda se puede ajustar según los cambios del servicio.

- Facturación flexible

  Los modos de pago por uso (según el uso del ancho de banda o la cantidad de tráfico) y de facturación anual/mensual están disponibles.

- Anchos de banda compartidos

  Los EIP pueden utilizar el ancho de banda compartido para reducir los costos de ancho de banda.

- Uso inmediato

  Las asociaciones y las desasociaciones de EIP, y los ajustes de ancho de banda entran en vigencia de inmediato.

3.2 Asignación de una EIP y vinculación de esta a un ECS

Escenarios

Puede asignar una EIP y vincularla a un ECS para que el ECS pueda acceder a Internet.

Asignación de una EIP

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En la página mostrada, haga clic en **Buy EIP**.
5. Establezca los parámetros como se le solicite.

Tabla 3-1 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Billing Mode	Los siguientes modos de facturación están disponibles: ● Anual/Mensual ● Pago por uso	Pay-per-use

Parámetro	Descripción	Valor de ejemplo
Region	Las regiones son áreas geográficas que están físicamente aisladas unas de otras. Las redes dentro de diferentes regiones no están conectadas entre sí, por lo que los recursos no se pueden compartir entre diferentes regiones. Para una menor latencia de red y un acceso más rápido a sus recursos, seleccione la región más cercana a usted. La región seleccionada para la EIP es su ubicación geográfica. **NOTA** La ubicación geográfica de una EIP comprada en CN North-Ulanqab1 es Pekín.	CN-Hong Kong
EIP Type	● **Dynamic BGP**: BGP dinámico proporciona conmutación por error automática y elige la ruta óptima cuando falla una conexión de red. ● **Static BGP**: BGP estático ofrece más control de enrutamiento y protege contra el flapping de ruta, pero no se puede seleccionar una ruta óptima en tiempo real cuando falla una conexión de red. ● **Premium BGP**: Premium BGP 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). (Este parámetro solo está disponible en CN-Hong Kong.)	Dynamic BGP

Parámetro	Descripción	Valor de ejemplo
Billed By	Este parámetro solo está disponible cuando se establece **Billing Mode** en **Pay-per-use**. ● **Bandwidth**: especifica un ancho de banda máximo y paga por la cantidad de tiempo que usa el ancho de banda. Esto es adecuado para escenarios con tráfico pesado o estable. ● **Traffic**: Usted especifica un ancho de banda máximo y paga por el tráfico total que usa. Esto es adecuado para escenarios con tráfico ligero o fuertemente fluctuante. ● **Shared Bandwidth**: El ancho de banda puede ser compartido por múltiples EIP. Esto es adecuado para escenarios con tráfico escalonado.	Bandwidth
Bandwidth	El tamaño del ancho de banda en Mbit/s.	100
EIP Name	El nombre de la EIP.	eip-test
Bandwidth Name	El nombre del ancho de banda.	bandwidth
Enterprise Project	El proyecto empresarial al que pertenece la EIP. Un proyecto empresarial facilita la gestión a nivel de proyectos y el agrupamiento de los recursos y usuarios en la nube. El nombre del proyecto predeterminado es **default**. .	default
Advanced Settings	Haga clic en la flecha desplegable para configurar los parámetros, incluidos el nombre y la etiqueta del ancho de banda.	-
Tag	Las etiquetas de la EIP. Cada etiqueta contiene un par de clave y valor. La clave y el valor de la etiqueta deben cumplir los requisitos enumerados en **Tabla 3-2**.	● Key: Ipv4_key1 ● Value: 192.168.12.10

Parámetro	Descripción	Valor de ejemplo
Monitoring	Se utiliza para monitorear la EIP. Habilitados por defect Puede utilizar la consola de gestión o las API proporcionadas por Cloud Eye para consultar las métricas y alarmas generadas para la EIP y el ancho de banda.	-
Required Duration	La duración durante la que utilizará la EIP adquirida. La duración debe especificarse si el **Billing Mode** está establecido en **Yearly/Monthly**.	1 month
Quantity	El número de las EIP que desea comprar. La cantidad debe especificarse si **Billing Mode** está establecido en **Pay-per-use**.	1

Tabla 3-2 Requisitos de la etiqueta EIP

Parámetro	Requerimientos	Valor de ejemplo
Clave	● No se puede dejar en blanco. ● Debe ser único para cada EIP. ● Puede contener un máximo de 36 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), y guiones (-).	Ipv4_key1
Value	● Puede contener un máximo de 43 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), puntos (.) y guiones (-).	192.168.12.10

NOTA

- Si está comprando una EIP facturada sobre una base de pago por uso y desea utilizar un ancho de banda compartido, solo puede seleccionar un ancho de banda compartido existente en la lista desplegable **Bandwidth Name**. Si no hay anchos de banda compartidos para seleccionar, compre primero un ancho de banda compartido.
- Un ancho de banda dedicado no se puede cambiar a un ancho de banda compartido y viceversa. Sin embargo, puede comprar ancho de banda compartido para las 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 del ancho de banda compartido, la EIP utilizará el ancho de banda dedicado.

6. Haga clic en **Next**.
7. Haga clic en **Submit**.

Vinculación de un EIP

1. En la página **EIPs**, busque la fila que contiene el EIP de destino y haga clic en **Bind**.
2. Seleccione la instancia a la que desea enlazar la EIP.
3. Haga clic en **OK**.

3.3 Desvinculación de un EIP desde un ECS y liberación del EIP

Escenarios

Si ya no necesita un EIP, desvíselo del ECS y libere el EIP para evitar desperdiciar recursos de red.

Notas y restricciones

- Solo puede liberar las EIP que no estén vinculadas a ningún recurso.
- No puede comprar una EIP que ha sido liberada si está actualmente en uso por otro usuario.
- El precio de una EIP de pago por uso incluye la tarifa de retención y el precio del ancho de banda. Si desvincula una EIP pero no la libera, se seguirá facturando a la EIP y el precio incluye la tarifa de retención y el precio del ancho de banda. En el momento en que vincula un EIP a una instancia, la tasa de retención ya no está incluida en el precio del EIP.

Procedimiento

Desvinculación de una sola EIP

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.

4. En la página mostrada, busque la fila que contiene la EIP de destino y haga clic en **Unbind**.
5. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Liberación de una sola EIP

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En la página mostrada, busque la fila que contiene la EIP de destino, haga clic en **More** y, a continuación, en **Release** en la columna **Operation**.
5. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Desvinculación de varias EIP a la vez

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En la página que se muestra, seleccione las EIP que desea no enlazar.
5. Haga clic en el botón **Unbind** situado encima de la lista de EIP.
6. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Liberación de varias EIP a la vez

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En la página mostrada, seleccione las EIP que se van a liberar.
5. Haga clic en el botón **Release** situado encima de la lista de EIP.
6. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

3.4 Modificación de un ancho de banda de EIP

Escenarios

Independientemente del modo de facturación que se utilice, si su EIP no se agrega a un ancho de banda compartido, utiliza un ancho de banda dedicado.

Esta sección describe cómo aumentar o disminuir un ancho de banda dedicado.

Cuando se cambia el tamaño del ancho de banda, el precio y el tiempo efectivo del ancho de banda varían según el modo de facturación, que se aplica a los anchos de banda dedicados y compartidos. Para más detalles, consulte **Tabla 3-3**.

Tabla 3-3 Impacto en la facturación después de un cambio de tamaño de ancho de banda

Modo de facturación	Facturación por	Cambio	Impacto
Anual/ Mensual	Ancho de banda	Aumentar el ancho de banda	El cambio entrará en vigor inmediatamente. El aumento del ancho de banda se facturará en consecuencia.
	Ancho de banda	Disminuir el ancho de banda al renovarse	El cambio no entrará en vigor inmediatamente. Debe seleccionar un nuevo tamaño de ancho de banda y una duración de renovación. El cambio entrará en vigor en el primer ciclo de facturación después de una renovación exitosa. ● La orden se puede cancelar antes de que el ancho de banda surta efecto. ● El ancho de banda no se puede modificar en el primer ciclo de facturación.
Pago por uso	Ancho de banda	Aumentar o disminuir el ancho de banda	El cambio entrará en vigor inmediatamente.
	Tráfico	Aumentar o disminuir el ancho de banda	El cambio entrará en vigor inmediatamente. El tamaño de ancho de banda que establezca solo se utiliza para limitar la velocidad máxima.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. Busque la fila que contenga la EIP objetivo en la lista de EIP, haga clic en **More** en la columna **Operation** (Operación) y seleccione Modify Bandwidth (Modificar ancho de banda).
5. Modifique los parámetros de ancho de banda según se le solicite.

Figura 3-2 Modificación del ancho de banda de un EIP de pago por uso

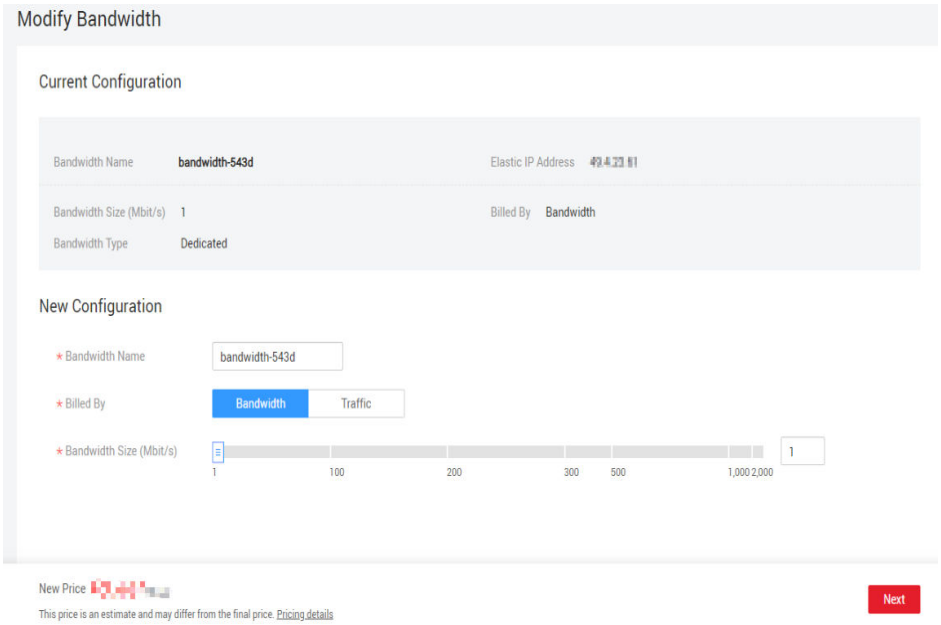
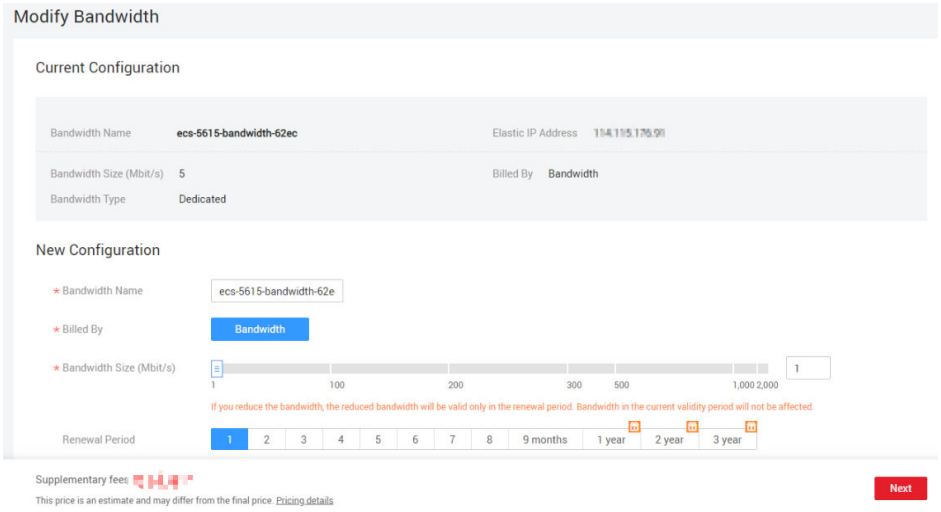


Figura 3-3 Modificación del ancho de banda mensual/anual



6. Haga clic en **Next**.
7. Haga clic en **Submit**.

3.5 Exportación de información de EIP

Escenarios

La información de todos los EIP de su cuenta se puede exportar en un archivo de Excel a un directorio local. El archivo registra el ID, el estado, el tipo, el nombre del ancho de banda y el tamaño del ancho de banda de los EIP.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En la página mostrada, haga clic en en la esquina superior derecha de la lista EIP.

   El sistema exportará automáticamente todos los EIP de la región actual de su cuenta a un archivo de Excel y descargará el archivo a un directorio local.

3.6 Gestión de etiquetas de EIP

Escenarios

Se pueden agregar etiquetas a los EIP para facilitar la identificación y gestión de los EIP. Puede agregar una etiqueta a un EIP al asignar el EIP. Alternativamente, puede agregar una etiqueta a un EIP asignado en la página de detalles de EIP. Se puede añadir un máximo de 10 etiquetas a cada EIP.

Una etiqueta consiste en un par clave y valor. **Tabla 3-4** enumera los requisitos de valor y clave de etiqueta.

Tabla 3-4 Requisitos de la etiqueta EIP

Parámetro	Requerimientos	Valor de ejemplo
Clave	● No se puede dejar en blanco. ● Debe ser único para cada EIP. ● Puede contener un máximo de 36 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), y guiones (-).	Ipv4_key1
Value	● Puede contener un máximo de 43 caracteres. ● Puede contener letras, dígitos, guiones bajos (_), puntos (.) y guiones (-).	192.168.12.10

Procedimiento

Búsqueda de EIP por clave de etiqueta y valor en la página que muestra la lista de EIP

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.

4. En la esquina superior derecha de la lista EIP, haga clic en **Search by Tag**.
5. En el área que se muestra, introduzca la clave de etiqueta y el valor del EIP que está buscando.

   Debe especificar tanto la clave de etiqueta como el valor. El sistema mostrará los EIP que contienen la etiqueta especificada.
6. Haga clic en + para agregar otra clave y valor de etiqueta.

   Se pueden agregar múltiples claves y valores de etiquetas para restringir los resultados de la búsqueda. Si agrega más de una etiqueta para buscar EIP, el sistema mostrará solo los EIP que contengan todas las etiquetas especificadas.
7. Haga clic en **Search**.

   El sistema muestra los EIP que está buscando en función de las claves de etiqueta y los valores introducidos.

Adición, eliminación, edición y consulta de etiquetas en la ficha Etiquetas de un EIP

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En la página mostrada, busque el EIP cuyas etiquetas desea gestionar y haga clic en el nombre del EIP.
5. En la página que muestra los detalles de EIP, haga clic en la ficha **Tags** y realice las operaciones deseadas en las etiquetas.
   - Consulte etiquetas.

     En la ficha **Tags**, puede ver detalles sobre las etiquetas agregadas al EIP actual, incluido el número de etiquetas y la clave y el valor de cada etiqueta.
   - Agregue una etiqueta.

     Haga clic en **Add Tag** en la esquina superior izquierda. En el cuadro de diálogo **Add Tag** que se muestra, escriba la clave y el valor de la etiqueta y haga clic en **OK**.
   - Edite una etiqueta.

     Busque la fila que contiene la etiqueta que desea editar y haga clic en **Edit** en la columna **Operation**. Escriba el nuevo valor de etiqueta y haga clic en **OK**.

     La clave de etiqueta no se puede modificar.
   - Elimine una etiqueta

     Busque la fila que contiene la etiqueta que desea eliminar y haga clic en **Delete** en la columna **Operation**. En la caja de diálogo que aparece, haga clic en **Yes**.

3.7 EIP de IPv6

Información general

Tanto IPv4 como IPv6 EIP están disponibles. Puede asignar un EIP IPv6 o asignar un EIP IPv4 existente a un EIP IPv6.

Una vez activada la función IPv6 EIP, obtendrá tanto un IPv4 EIP como su IPv6 EIP correspondiente. Las direcciones IPv6 externas pueden acceder a los recursos en la nube a través de esta EIP IPv6.

Los EIP IPv4 se facturan. Los EIP de IPv6 son actualmente gratuitos, pero se facturarán en una fecha posterior (el precio aún no se ha determinado).

Escenarios de aplicación de doble pila IPv4/IPv6

Si su ECS admite IPv6, puede utilizar la pila dual IPv4/IPv6. **Tabla 3-5** muestra los escenarios de aplicación de ejemplo.

Tabla 3-5 Escenarios de aplicación de doble pila IPv4/IPv6

Escenario de la aplicación	Descripción	Requisito	Subred IPv4 o IPv6	ECS
Comunicación IPv4 privada	Sus aplicaciones en ECS necesitan comunicarse con otros sistemas (como bases de datos) a través de direcciones IPv4 privadas.	● IPv6 no está habilitado para la subred de VPC. ● Ninguno EIP ha estado vinculado a los ECS.	Bloque CIDR IPv4	**Private IPv4 address**: utilizada para la comunicación IPv4 privada.
Comunicación IPv4 pública	Sus aplicaciones en ECS necesitan comunicarse con otros sistemas (como bases de datos) a través de direcciones IPv4 públicas.	● IPv6 no está habilitado para la subred de VPC. ● Los EIP han estado vinculados a los ECS.	Bloque CIDR IPv4	● **Private IPv4 address**: utilizada para la comunicación IPv4 privada. ● **Public IPv4 address**: utilizada para la comunicación IPv4 pública.

Escenario de la aplicación	Descripción	Requisito	Subred IPv4 o IPv6	ECS
Comunicación IPv6 privada	Sus aplicaciones en ECS necesitan comunicarse con otros sistemas (como bases de datos) a través de direcciones IPv6 privadas.	• Se ha habilitado IPv6 para la subred de VPC. • La red se ha configurado para los ECS de la siguiente manera: – **VPC and Subnet**: subred y VPC habilitados para IPv6. – **Self-assigned IPv6 address**: Seleccionada. – **Shared Bandwidth**: seleccionado **Do not configure**.	• Bloque CIDR IPv4 • Bloque CIDR IPv6	• **Private IPv4 address + IPv4 EIP**: Enlaza un IPv4 EIP a la instancia para permitir la comunicación IPv4 pública. • **Private IPv4 address**: no enlaza ningún EIP IPv4 a la instancia y utilice únicamente la dirección IPv4 privada para permitir la comunicación IPv4 privada. • **IPv6 address**: No configure el ancho de banda compartido para la dirección IPv6 para permitir la comunicación IPv6 privada.

Escenario de la aplicación	Descripción	Requisito	Subred IPv4 o IPv6	ECS
Comunicación IPv6 pública	Se requiere una red IPv6 para que el ECS acceda al servicio IPv6 en Internet.	• Se ha habilitado IPv6 para la subred de VPC. • La red se ha configurado para los ECS de la siguiente manera: – **VPC and Subnet**: subred y VPC habilitados para IPv6. – **Self-assigned IPv6 address**: Seleccionada. – **Shared Bandwidth**: Se ha seleccionado un ancho de banda compartido.	• Bloque CIDR IPv4 • Bloque CIDR IPv6	• **Private IPv4 address + IPv4 EIP**: Enlaza un IPv4 EIP a la instancia para permitir la comunicación IPv4 pública. • **Private IPv4 address**: no enlaza ningún EIP IPv4 a la instancia y utilice únicamente la dirección IPv4 privada para permitir la comunicación IPv4 privada. • **IPv6 address + shared bandwidth**: Permite la comunicación IPv6 privada y la comunicación IPv6 pública.

Escenarios de aplicación de IPv6 EIP

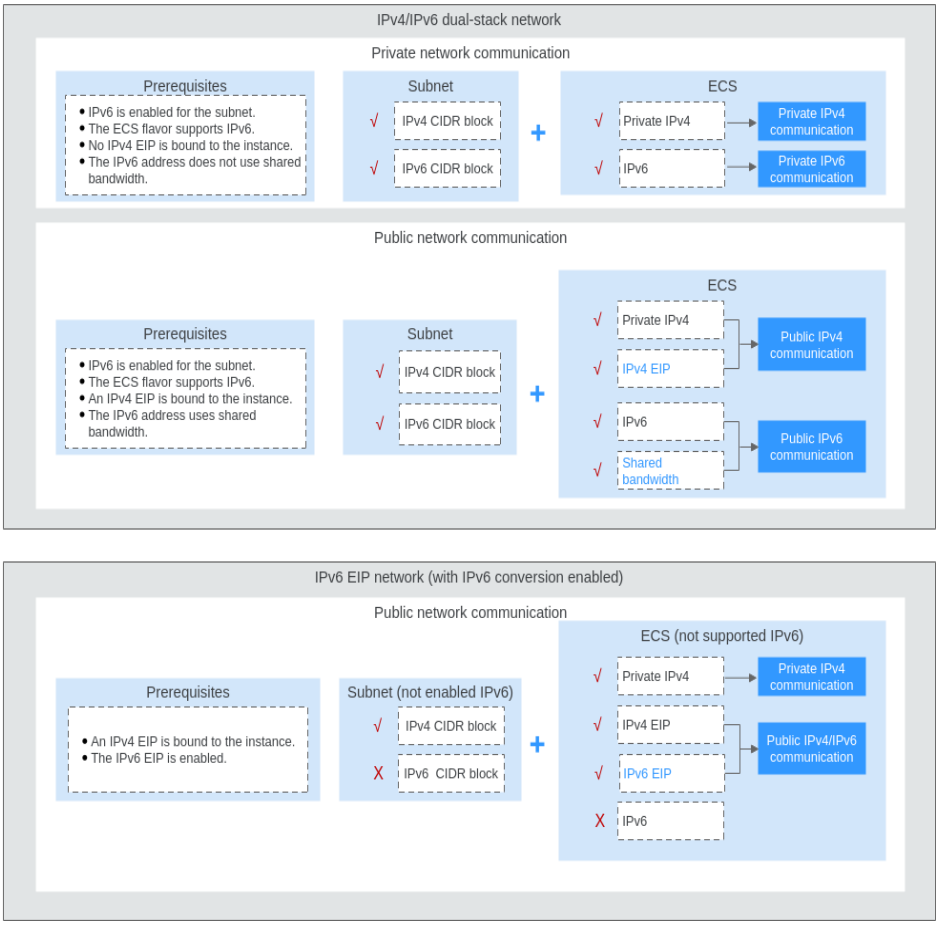
Si desea que un ECS proporcione servicios IPv6 pero el ECS no admite redes IPv6 o no desea crear una red IPv6, puede usar IPv6 EIP para abordar rápidamente sus requisitos. Para obtener más información sobre los escenarios de la aplicación y la planificación de recursos, consulte **Tabla 3-6**.

Tabla 3-6 Escenarios de aplicación y planificación de recursos de una red IPv6 EIP (con IPv6 EIP habilitado)

Escenario de la aplicación	Descripción	Requisito	Subred IPv4 o IPv6	ECS
Comunicación IPv6 pública	Desea permitir que un ECS proporcione servicios IPv6 para clientes en Internet sin configurar una red IPv6.	• Un EIP ha sido vinculado al ECS. • IPv6 EIP ha sido habilitado.	Bloque CIDR IPv4	• **Private IPv4 address**: utilizada para la comunicación IPv4 privada. • **IPv4 EIP (with IPv6 EIP enabled)**: utilizado para la comunicación de red pública a través de direcciones IPv4 e IPv6.

Escenarios de aplicaciones y planificación de recursos de redes IPv6

Figura 3-4 Escenarios de aplicaciones y planificación de recursos de redes IPv6



Habilitación de IPv6 (asignación de EIP de IPv6)

- Método 1:

  Seleccione la opción **IPv6 EIP** cuando asigne una EIP haciendo referencia a **Asignación de una EIP y vinculación de esta a un ECS** para que pueda obtener una EIP de IPv4 y de IPv6.

  Las direcciones de IPv6 externas pueden acceder a los recursos de la nube a través de esta EIP de IPv6.

- Método 2:

  Si desea un EIP IPv6 además de un EIP IPv4 existente, busque la fila que contiene el EIP IPv4 de destino, haga clic en **More** en la columna **Operation** y seleccione **Enable IPv6 EIP**. A continuación, se asignará un EIP IPv6 correspondiente y

  Una vez habilitado el IPv6 EIP, obtendrá tanto un IPv4 EIP como un IPv6 EIP. Las direcciones IPv6 externas pueden acceder a los recursos en la nube a través de esta EIP IPv6.

NOTA

no se producen efectos adversos en los recursos en la nube vinculados a las EIP IPv4 existentes.

Configuración de grupos de seguridad

Después de que IPv6 EIP esté habilitado, agregue reglas de grupo de seguridad entrantes y salientes para permitir paquetes hacia y desde el rango de direcciones IP **198.19.0.0/16**. **Tabla 3-7** muestra las reglas del grupo de seguridad. IPv6 EIP utiliza NAT64 para convertir la dirección IP de origen en la dirección entrante en una dirección IPv4 en el rango de direcciones IP 198.19.0.0/16. El puerto de origen puede ser aleatorio, la dirección IP de destino es la dirección IPv4 privada de su servidor local, y el puerto de destino permanece sin cambios.

Tabla 3-7 Reglas de grupos de seguridad

Dirección	Protocolo	Origen o destino
Entrante	Todos	Fuente: 198.19.0.0/16
Saliente	Todos	Destino: 198.19.0.0/16

Desactivación de IPv6 EIP

Si no necesita el EIP IPv6, busque la fila que contiene su EIP IPv4 correspondiente, haga clic en **More** en la columna **Operation** y seleccione **Disable IPv6 EIP**. A continuación, se liberará el EIP IPv6. Solo tendrá el IPv4 EIP.

4 Anchos de banda compartidos

4.1 Descripción general del ancho de banda compartido

Un ancho de banda compartido puede ser compartido por múltiples EIP y controla la velocidad de transferencia de datos en estos EIP de una manera centralizada. Todos los ECS, BMS y balanceadores de carga que tienen EIP enlazados en la misma región pueden compartir un ancho de banda.

Cuando aloja un gran número de aplicaciones en la nube, si cada EIP utiliza un ancho de banda independiente, se requieren muchos anchos de banda, lo que aumenta significativamente los costos de ancho de banda. Si todos los EIP comparten el mismo ancho de banda, puede reducir el costo de ancho de banda y realizar fácilmente el sistema O&M.

- Reducción de los costos de ancho de banda

  El uso compartido y la multiplexación del ancho de banda a nivel regional reducen el uso del ancho de banda y los costes de operación y mantenimiento.
- Operaciones flexibles

  Puede agregar EIP que se facturan de forma de pago por uso a un ancho de banda compartido o eliminarlos de un ancho de banda compartido independientemente de los tipos de EIP y las instancias a las que estén vinculados.
- Modos de facturación flexibles

  Se proporcionan los modos de facturación anual/mensual y de pago por uso.

Notas y restricciones

- El tamaño mínimo de un ancho de banda compartido que se puede comprar es de 5 Mbit/s. Solo puede agregar EIP de pago por uso a un ancho de banda compartido.
- Cada cuenta puede tener un máximo de 5 anchos de banda compartidos. Si necesita más anchos de banda compartidos, envíe un ticket de servicio para solicitar un aumento de cuota.
- Si se elimina un ancho de banda compartido anual/mensual al expirar, los EIP que comparten el ancho de banda se eliminarán del ancho de banda y se facturarán en función del modo antes de agregarlos al ancho de banda compartido.
- Un ancho de banda compartido no puede controlar el límite de transferencia de datos en una única EIP. La velocidad de transferencia de datos en los EIP no se puede personalizar.

- Un ancho de banda compartido solo puede ser utilizado por los recursos de su misma cuenta.

  NOTA

  - Un ancho de banda dedicado no se puede cambiar a un ancho de banda compartido y viceversa. Sin embargo, puede comprar un ancho de banda compartido para EIP de pago por uso.
    - Agregue un EIP a un ancho de banda compartido y, a continuación, el EIP utilizará el ancho de banda compartido.
    - Retire el EIP del ancho de banda compartido y, a continuación, el EIP utilizará el ancho de banda dedicado.

4.2 Asignación de un ancho de banda compartido

Escenarios

Cuando aloja un gran número de aplicaciones en la nube, si cada EIP utiliza un ancho de banda dedicado, se requieren muchos anchos de banda, lo que conlleva altos costos. Si todos los EIP comparten el mismo ancho de banda, los costos de operación de la red se reducirán y su sistema O&M, así como las estadísticas de recursos se simplificarán.

Asigne un ancho de banda compartido para su uso con EIP.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. En la esquina superior derecha, haz clic en **Buy Shared Bandwidth**. En la página mostrada, configure los parámetros según se le solicite.

Tabla 4-1 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Billing Mode	El modo de facturación de un ancho de banda compartido. El modo de facturación puede ser: ● Anual/Mensual: Usted paga por el ancho de banda por año o mes antes de usarlo. No se aplican otros cargos durante el período de validez del ancho de banda. ● Pago por uso: Usted paga por el ancho de banda en función de la cantidad de tiempo que usa el ancho de banda.	Yearly/Monthly

Parámetro	Descripción	Valor de ejemplo
Region	Las regiones son áreas geográficas que están físicamente aisladas unas de otras. Las redes dentro de diferentes regiones no están conectadas entre sí, por lo que los recursos no se pueden compartir entre diferentes regiones. Para una menor latencia de red y un acceso más rápido a sus recursos, seleccione la región más cercana a usted.	CN-Hong Kong
Billed By	El método de facturación para el ancho de banda compartido. La facturación puede ser por ancho de banda.	Bandwidth
Bandwidth	El tamaño del ancho de banda en Mbit/s. El valor mínimo es 5 Mbit/s. El ancho de banda máximo puede ser 2000 Mbit/s.	10
Enterprise Project	El proyecto de empresa al que pertenece la EIP. Un proyecto empresarial facilita la gestión a nivel de proyectos y el agrupamiento de los recursos y usuarios en la nube. El nombre del proyecto predeterminado es **default**.	default
Bandwidth Name	El nombre del ancho de banda compartido.	Bandwidth-001
Required Duration	La duración durante la que utilizará la EIP adquirida. La duración debe especificarse si el **Billing Mode** está establecido en **Yearly/ Monthly**.	2 months

6. Haga clic en **Next**.

4.3 Adición de EIP a un ancho de banda compartido

Escenarios

Agrega las EIP a un ancho de banda compartido y las EIP pueden compartir ese ancho de banda. Puede agregar varias EIP a un ancho de banda compartido al mismo tiempo.

Notas y restricciones

- Actualmente, las EIP anuales/mensuales no se pueden agregar a un ancho de banda compartido.
- Después de agregar una EIP a un ancho de banda compartido, el ancho de banda original utilizado por la EIP no será válida y la EIP comenzará a utilizar el ancho de banda compartido.
- El ancho de banda dedicado original de la EIP se eliminará y ya no se facturará.

- Para agregar una EIP anual/mensual a un ancho de banda compartido, primero debe cambiar su modo de facturación a pago por uso.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. En la lista de ancho de banda compartido, busque la fila que contiene el ancho de banda compartido al que desea agregar las EIP. En la columna **Operation**, elija **Add EIP**, y seleccione las EIP que se van a agregar.
6. Haga clic en **OK**.

4.4 Eliminación de EIP de un ancho de banda compartido

Escenarios

Elimine los EIP que ya no son necesarios de un ancho de banda compartido si es necesario.

Notas y restricciones

No se puede eliminar un EIP anual/mensual de un ancho de banda compartido adquirido durante la OBT.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. En la lista de ancho de banda compartido, busque la fila que contiene el ancho de banda del que se van a eliminar los EIP, elija **More** > **Remove EIP** en la columna **Operation**, y seleccione los EIP que se van a eliminar en el cuadro de diálogo que se muestra.
6. Establezca el ancho de banda del EIP después de eliminar el EIP. Puede configurar el modo de facturación EIP y el tamaño del ancho de banda.
7. Haga clic en **OK**.

4.5 Modificación de un ancho de banda compartido

Escenarios

Puede modificar el nombre y el tamaño de un ancho de banda compartido según sea necesario.

- Si un ancho de banda compartido se factura sobre una base de pago por uso, la modificación entrará en vigor inmediatamente. Para más detalles, consulte **Modificación de un ancho de banda compartido (pago por uso)**.
- Si un ancho de banda compartido se factura anualmente/mensualmente:
  - **puede aumentar el ancho de banda.** El aumento del tamaño del ancho de banda tendrá efecto inmediatamente y la diferencia de precio se facturará en consecuencia.
  - **puede reducir el ancho de banda.** El tamaño reducido del ancho de banda tendrá efecto en el primer ciclo de facturación después de una renovación exitosa.

Modificación de un ancho de banda compartido (pago por uso)

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. En la lista de ancho de banda compartido, busque la fila que contiene el ancho de banda compartido que desea modificar, haga clic en **Modify Bandwidth** en la columna **Operation** y modifique la configuración de ancho de banda.
6. Haga clic en **Next**.
7. Haga clic en **Submit**.

   La modificación entra en vigor inmediatamente.

Aumento del ancho de banda compartido (anual/mensual)

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. En la lista de ancho de banda compartido, busque la fila que contiene el ancho de banda compartido de destino y haga clic en **Modify Bandwidth** en la columna **Operation**.
6. Seleccione **Increase bandwidth** y haga clic en **Continue**.
7. En el área **New Configuration** de la página **Modify Bandwidth**, cambie el nombre y el tamaño del ancho de banda.

8. Haga clic en **Next**.
9. Confirme la información y haga clic en **Pay Now**.

   Después de completar el pago, el aumento de ancho de banda entrará en vigor inmediatamente.

Disminución de un ancho de banda compartido (anual/mensual)

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. En la lista de ancho de banda compartido, busque la fila que contiene el ancho de banda compartido de destino y haga clic en **Modify Bandwidth** en la columna **Operation**.
6. Seleccione **Decrease bandwidth** y haga clic en **Continue**.
7. En el área **New Configuration** de la página **Modify Bandwidth**, cambie el nombre y el tamaño del ancho de banda.
8. Haga clic en **Next**.
9. Confirme la información y haga clic en **Pay Now**.

   Después de completar el pago, el ancho de banda reducido entrará en vigor en el primer ciclo de facturación después de que finalice la suscripción actual.

4.6 Eliminación de un ancho de banda compartido

Escenarios

Elimine un ancho de banda compartido facturado sobre una base de pago por uso si ya no es necesario.

Notas y restricciones

Un ancho de banda compartido anual/mensual no se puede eliminar directamente. Si desea cancelar la suscripción, acceda al Centro de usuarios.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. En el panel de navegación de la izquierda, elija **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. En la lista de ancho de banda compartido, busque la fila que contiene el ancho de banda compartido de pago por uso que desea eliminar, haga clic en **More** en la columna **Operation** y, a continuación, haga clic en **Delete**.

6. En la caja de diálogo que aparece, haga clic en **Yes**.

5 Paquete de datos compartidos

5.1 Descripción general del paquete de datos compartidos

El paquete de datos compartido proporciona una cuota para el uso de datos. Tales envases son rentables y fáciles de usar. Los paquetes de datos compartidos entran en vigor inmediatamente después de su compra. Si se ha suscrito a EIP de pago por uso utilizando el ancho de banda facturado por tráfico en una región y compra un paquete de datos compartidos en la misma región, los EIP utilizarán el paquete de datos compartidos. Una vez que la cuota del paquete se agote o que el paquete venza, los EIP se seguirán facturando en modo de pago por uso.

- Hay dos tipos de paquetes disponibles: BGP dinámico y BGP estático. Los paquetes de datos BGP dinámicos serán utilizados por los EIPs BGP dinámicos, y los paquetes de datos BGP estáticos serán utilizados por los EIPs BGP estáticos.
- Los paquetes de datos compartidos se pueden comprar anualmente o mensualmente. Los paquetes comprados por un año son más rentables. Puede comprar varios paquetes de datos compartidos. El paquete de datos con el período de validez más corto se utilizará primero.

Notas y restricciones

- Un paquete de datos compartido solo tiene efecto para el ancho de banda facturado por el tráfico. Hay disponibles dos tipos de paquetes de datos compartidos: BGP estático (para ancho de banda BGP estático) y BGP dinámico (para ancho de banda BGP dinámico).
- Un paquete de datos compartido no puede surtir efecto para el ancho de banda de un EIP específico.
- Un paquete de datos compartido no puede tener efecto para un ancho de banda compartido.
- Los EIP del tipo BGP premium no pueden utilizar un paquete de datos compartido.
- No se puede cancelar la suscripción a un paquete de datos compartido.

5.2 Compra de un paquete de datos compartidos

Scenarios

This section describes how to buy a shared data package. Shared data packages take effect immediately after your purchase. If you have subscribed to pay-per-use EIPs billed by traffic in a region and buy a shared data package in the same region, the EIPs will use the shared data package. After the package quota is used up or the package expires, the EIPs will continue to be billed on a pay-per-use basis.

Notas y restricciones

- Un paquete de datos compartido solo tiene efecto para el ancho de banda facturado por el tráfico. Hay disponibles dos tipos de paquetes de datos compartidos: BGP estático (para ancho de banda BGP estático) y BGP dinámico (para ancho de banda BGP dinámico).
- Un paquete de datos compartido no puede surtir efecto para el ancho de banda de un EIP específico.
- Un paquete de datos compartido no puede tener efecto para un ancho de banda compartido.
- Los EIP del tipo BGP premium no pueden utilizar un paquete de datos compartido.
- No se puede cancelar la suscripción a un paquete de datos compartido.

Procedure

1. Log in to the management console.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Data Packages**.
5. In the upper right corner, click **Buy Shared Data Package**. On the displayed page, configure parameters as prompted.

Tabla 5-1 Parameter descriptions

Parameter	Description	Example Value
Region	A shared data package can only be used by resources in its same region. Select the region based on your requirements.	CN-Hong Kong

Parameter	Description	Example Value
Type	The shared data package type. Set this parameter based on the bandwidth type of the EIP. The following two types of packages are available: ● Dynamic BGP: A dynamic BGP data package can only be used by dynamic BGP EIPs billed by traffic on a pay-per-use basis. ● Static BGP: A static BGP data package can only be used by static BGP EIPs billed by traffic on a pay-per-use basis.	Static BGP
Package Validity	The validity period of the shared data package. Select a validity period based on service requirements. A shared data package cannot be unsubscribed and takes effect immediately after you purchase it. Expired shared data packages will longer be available for use.	1 month
Specification	The size of the shared data package in GB.	10 GB
Usage Duration	The validity period of the shared data package.	Default

6. Click **Next**.

6 Tabla de ruta

6.1 Descripción general de la tabla de ruta

Tabla de rutas

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. Cada subred 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 a la misma tabla de ruta.

Tabla de rutas predeterminada y tabla de rutas personalizadas

Cuando se crea una VPC, el sistema genera automáticamente una tabla de ruta predeterminada para la VPC. Si crea una subred en la VPC, la subred se asocia automáticamente a la tabla de rutas predeterminada.

- Puede agregar rutas a, eliminar rutas de y modificar rutas en la tabla de rutas predeterminada, pero no puede eliminar la tabla.
- Cuando creas una conexión de VPN, de Cloud Connect, o de Direct Connect, la tabla de rutas predeterminada entrega automáticamente una ruta que no se puede eliminar ni modificar.

Si no desea utilizar la tabla de rutas predeterminada, ahora puede crear una tabla de rutas personalizada y asociarla a la subred. Puede eliminar la tabla de ruta personalizada si ya no es necesaria.

NOTA

- La tabla de ruta personalizada asociada a una subred afecta sólo al tráfico saliente. La tabla de ruta predeterminada determina el tráfico entrante.
- Para utilizar una tabla de rutas personalizada, debe enviar un ticket de servicio. Debe hacer clic en **Increase quota** en la página **Create Route Table** o elegir **More** > **Service Tickets** > **Create Service Ticket** en la esquina superior derecha de la página. Para obtener más información, consulte **Enviar un ticket de servicio**.

Para obtener más información sobre cómo crear una tabla de rutas personalizada, consulte la sección **Creación de una tabla de ruta personalizada**.

Ruta

Una ruta se configura con el destino, el tipo de salto siguiente y el salto siguiente para determinar a dónde se dirige el tráfico de red. Las rutas se clasifican en las rutas del sistema y las rutas personalizadas.

- Rutas del sistema: Estas rutas son agregadas automáticamente por el sistema y no se pueden modificar o eliminar.

  Después de crear una tabla de rutas, el sistema agrega automáticamente las siguientes rutas de sistema a la tabla de rutas, para que las instancias de una VPC puedan comunicarse entre sí.

  – Rutas cuyo destino es 100.64.0.0/10 o 198.19.128.0/20.

  – Rutas cuyo destino es un bloque CIDR de subred.

  > NOTA
  >
  > Además de las rutas del sistema anteriores, el sistema agrega automáticamente una ruta cuyo destino es 127.0.0.0/8. Esta es la dirección de bucle de retorno local.
  >
  > Tanto las rutas del sistema como las personalizadas son rutas BGP estáticas.

- Rutas personalizadas: Estas son rutas que puede agregar, modificar y eliminar. El destino de una ruta personalizada no se puede superponer al de una ruta de sistema.

  Puede agregar una ruta personalizada y configurar el destino, el tipo de salto siguiente y el salto siguiente en la ruta para determinar a dónde se dirige el tráfico de red. **Tabla 6-1** enumera los tipos admitidos de saltos siguientes.

Tabla 6-1 Tipo del próximo salto

Tipo del próximo salto	Descripción	Tabla de rutas admitida
Servidor	El tráfico dirigido hacia el destino es reenviado a un ECS en la VPC.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
NIC de extensión	El tráfico dirigido hacia el destino es reenviado a una NIC de extensión de un ECS en la VPC.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Red definida por el usuario de BMS	El tráfico destinado al destino se reenvía a una red de BMS definida por el usuario.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Gateway de la VPN	El tráfico dirigido hacia el destino es reenviado a un VPN Gateway.	Tabla de rutas personalizada
Gateway de Direct Connect	El tráfico dirigido hacia el destino es reenviado a un Direct Connect Gateway.	Tabla de rutas personalizada

Tipo del próximo salto	Descripción	Tabla de rutas admitida
Cloud connection	Traffic intended for the destination is forwarded to a cloud connection.	Tabla de rutas personalizada
Interfaz de red suplementaria	El tráfico dirigido hacia el destino se reenvía a la interfaz de red suplementaria de un ECS en la VPC.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Gateway de NAT	El tráfico dirigido hacia el destino es reenviado a un NAT Gateway.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Interconexión de VPC	El tráfico dirigido hacia el destino es reenviado a una interconexión de VPC.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Dirección IP virtual	El tráfico dirigido hacia el destino se reenvía a una dirección IP virtual y luego es enviado a los ECS activos y en standby a los que está vinculada la dirección IP virtual.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Enrutador empresarial	El tráfico destinado al destino se reenvía a un enrutador empresarial.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Firewall en la nube	El tráfico destinado al destino se reenvía a un firewall en la nube.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada

NOTA

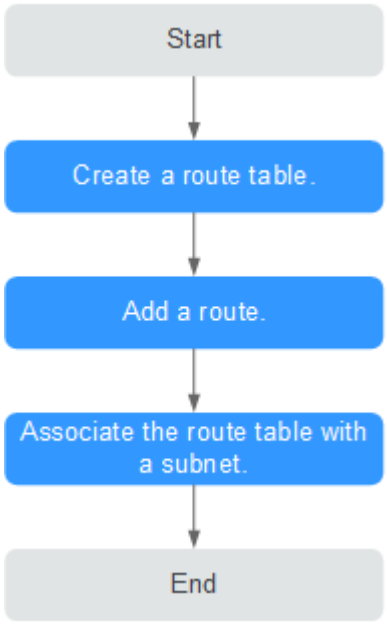
Si especifica el destino al crear un recurso, se entrega una ruta del sistema. Si no especifica un destino al crear un recurso, se entrega una ruta personalizada que se puede modificar o eliminar.

Por ejemplo, cuando se crea un gateway de NAT, el sistema entrega automáticamente una ruta personalizada sin un destino específico (0.0.0.0/0 se utiliza de forma predeterminada). En este caso, puede cambiar el destino. Sin embargo, cuando crea un gateway de VPN, debe especificar la subred remota, es decir, el destino de una ruta. En este caso, el sistema entrega esta ruta del sistema. No modifique el destino de la ruta en la página **Route Tables**. Si lo hace, el destino no será coherente con la subred remota configurada. Para modificar el destino de la ruta, vaya a la página de recursos específica y modifique la subred remota, a continuación, el destino de la ruta se cambiará en consecuencia.

Proceso de configuración de tabla de ruta personalizada

Figura 6-1 muestra el proceso de creación y configuración de una tabla de ruta personalizada.

Figura 6-1 Proceso de configuración de tabla de rutas



1. Para obtener más información sobre cómo crear una tabla de enrutamiento personalizada, consulte **Creación de una tabla de ruta personalizada**.
2. Para obtener más información sobre cómo agregar una ruta personalizada, consulte **Adición de una ruta personalizada**.
3. Para obtener más información acerca de cómo asociar una subred a una tabla de rutas, consulte **Asociar una subred a una tabla de ruta**. Después de la asociación, las rutas en la tabla de rutas controlan el enrutamiento para la subred.

Notas y restricciones

- Cuando se crea una VPC, el sistema genera automáticamente una tabla de ruta predeterminada para la VPC.
- Se puede agregar un máximo de 200 rutas a cada tabla de rutas.
- No se puede eliminar la tabla de rutas predeterminada.
- La ruta del sistema no se puede modificar ni eliminar.
- Las rutas entregadas por los servicios VPN, Cloud Connect y Direct Connect a la tabla de rutas predeterminada no se pueden modificar ni eliminar.

6.2 Creación de una tabla de ruta personalizada

Escenarios

Puede crear una tabla de rutas personalizada si no desea utilizar la predeterminada.

Para utilizar una tabla de rutas personalizada, debe enviar un ticket de servicio. Debe hacer clic en **Increase quota** en la página **Create Route Table** o elegir **More** > **Service Tickets** > **Create Service Ticket** en la esquina superior derecha de la página.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la esquina superior derecha, haga clic en **Create Route Table**. En la página mostrada, configure los parámetros según se le solicite.

   Tabla 6-2 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	Nombre de la tabla de rutas. Este parámetro es obligatorio. El nombre puede contener un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios.	rtb-001
VPC	La VPC a la que pertenece la tabla de ruta. Este parámetro es obligatorio.	vpc-001
Description	Información complementaria sobre la tabla de rutas. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-
Route Settings	La información de la ruta. Este parámetro es opcional. Puede agregar una ruta al crear la tabla de rutas o después de crear la tabla de rutas. Para más detalles, consulte **Adición de una ruta personalizada**. Puedes hacer clic en + para agregar más rutas.	-

6. Haga clic en **OK**.

   Se muestra un mensaje. Puede determinar si desea asociar la tabla de ruta a las subredes inmediatamente como se le solicite. Si desea asociar inmediatamente, realice las siguientes operaciones:

   a. Haga clic en **Associate Subnet**. Se muestra la página de detalles de la tabla de rutas.
   b. Haga clic en **Associate Subnet** y seleccione las subredes de destino que se van a asociar.
   c. Haga clic en **OK**.

6.3 Asociar una subred a una tabla de ruta

Escenarios

Después de asociar una tabla de rutas a una subred, las rutas de la tabla de rutas controlan el enrutamiento de la subred y se aplican a todos los recursos de nube de la subred. Determine el impacto de los servicios antes de realizar esta operación.

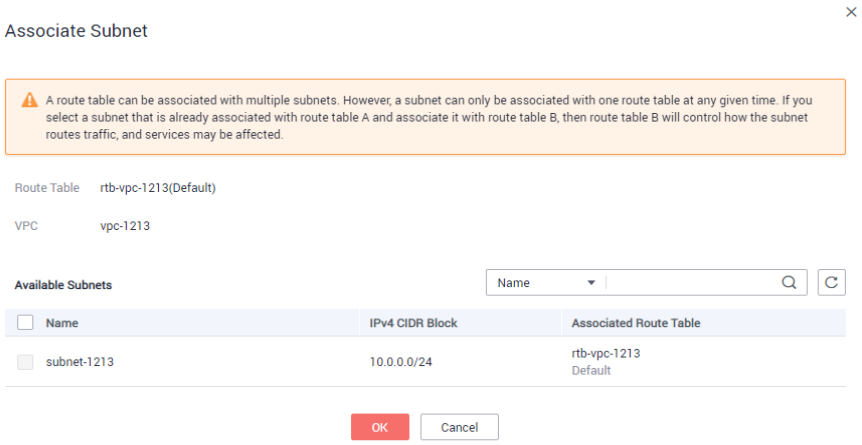
Notas y restricciones

Una subred sólo se puede asociar a una tabla de ruta.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, busque la fila que contiene la tabla de rutas de destino y haga clic en **Associate Subnet** en la columna **Operation**.
6. Seleccione la subred que desea asociar.

   Figura 6-2 Asociar subred



7. Haga clic en **OK**.

6.4 Cambio de la tabla de ruta asociada a una subred

Escenarios

Puede cambiar la tabla de rutas asociada a la subred a otra en la VPC. Si se cambia la tabla de enrutamiento de una subred, las rutas de la tabla de enrutamiento nuevas se aplicarán a todos

los recursos en la nube de la subred. Determine el impacto de los servicios antes de realizar esta operación.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, haga clic en el nombre de la tabla de rutas de destino.
6. En la página de la ficha **Associated Subnets**, haga clic en **Change Route Table** en la columna **Operation** y seleccione una nueva tabla de ruta según se le solicite.
7. Haga clic en **OK**.

   Después de cambiar la tabla de rutas para una subred, las rutas de la nueva tabla de rutas se aplicarán a todos los recursos de nube de la subred.

6.5 Consulta de una tabla de rutas

Escenarios

Puede ver la información básica, las rutas y las subredes asociadas de una tabla de rutas.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, haga clic en el nombre de la tabla de rutas de destino.

6.6 Exportación de información de tabla de ruta

Escenarios

La información sobre todas las tablas de rutas de su cuenta se puede exportar como un archivo de Excel a un directorio local. Este archivo registra el nombre, ID, VPC, tipo y número de subredes asociadas de las tablas de ruta.

Procedimiento

1. Inicie sesión en la consola de gestión.

2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la página mostrada, haga clic en en la parte superior derecha de la lista de tablas de rutas.

   El sistema exportará automáticamente información sobre todas las tablas de rutas de su cuenta en la región actual como un archivo de Excel a un directorio local.

6.7 Supresión de una tabla de ruta

Escenarios

Puede eliminar las tablas de ruta personalizadas pero no puede eliminar la tabla de rutas predeterminada.

Prerrequisitos

Antes de eliminar una tabla de rutas, asegúrese de que no se ha asociado ninguna subred a la tabla de rutas personalizada. Si hay una subred asociada, asocie la subred a otra tabla de ruta haciendo clic en **Change Route Table** y, a continuación, elimine la tabla de ruta personalizada.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, busque la fila que contiene la tabla de rutas que se va a eliminar y haga clic en **Delete** en la columna **Operation**.
6. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

6.8 Adición de una ruta personalizada

Escenarios

Cada tabla de rutas contiene una ruta de sistema predeterminada, que indica que los ECS de una VPC pueden comunicarse entre sí. Puede agregar rutas personalizadas según sea necesario para reenviar el tráfico destinado al destino al salto siguiente especificado.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, haga clic en el nombre de la tabla de rutas a la que desea agregar una ruta.
6. Haga clic en **Add Route** y defina los parámetros según se le solicite.

   Puedes hacer clic en + para agregar más rutas.

Figura 6-3 Agregar ruta

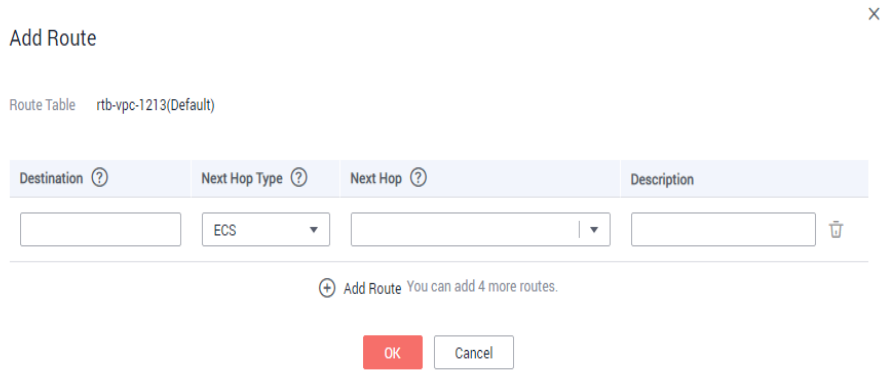


Tabla 6-3 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Destination	El bloque CIDR de destino. El destino de cada ruta debe ser único. El destino no se puede superponer con ningún bloque CIDR de subred en la VPC.	192.168.0.0/16
Next Hop Type	Establezca el tipo de salto siguiente. Para obtener más información sobre los tipos de recursos admitidos, consulte **Tabla 6-1**. **NOTA** Cuando agrega o modifica una ruta personalizada en una tabla de rutas predeterminada, el tipo de salto siguiente de la ruta no se puede establecer en **VPN gateway**, **Direct Connect gateway**, o **Cloud connection**.	ECS
Next Hop	Ajuste el salto siguiente. Los recursos del cuadro de lista desplegable se muestran en función del tipo de salto siguiente seleccionado.	ecs-001

Parámetro	Descripción	Valor de ejemplo
Description	Información complementaria sobre la ruta. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

7. Haga clic en **OK**.

6.9 Modificación de una ruta

Escenarios

Modificar una ruta existente.

Notas y restricciones

- La ruta del sistema no se puede modificar.
- Las rutas entregadas por los servicios VPN, Direct Connect y Cloud Connect a la tabla de rutas predeterminada no se pueden modificar.In addition, the route of a gateway VPC endpoint in the custom route table cannot be modified.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, haga clic en el nombre de la tabla de rutas de destino.
6. Busque la fila que contiene la ruta que se va a modificar y haga clic en **Modify** en la columna **Operation**.
7. Modifique la información de ruta en el cuadro de diálogo mostrado.

Tabla 6-4 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Destination	El bloque CIDR de destino. El destino de cada ruta debe ser único. El destino no se puede superponer con ningún bloque CIDR de subred en la VPC.	192.168.0.0/16

Parámetro	Descripción	Valor de ejemplo
Next Hop Type	Establezca el tipo de salto siguiente. Para obtener más información sobre los tipos de recursos admitidos, consulte **Tabla 6-1**. **NOTA** Cuando agrega o modifica una ruta personalizada en una tabla de rutas predeterminada, el tipo de salto siguiente de la ruta no se puede establecer en **VPN gateway**, **Direct Connect gateway**, o **Cloud connection**.	ECS
Next Hop	Ajuste el salto siguiente. Los recursos del cuadro de lista desplegable se muestran en función del tipo de salto siguiente seleccionado.	ecs-001
Description	Información complementaria sobre la ruta. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

8. Haga clic en **OK**.

6.10 Replicación de una ruta

Escenarios

Esta sección describe cómo replicar las rutas entre todas las tablas de rutas de una VPC. Las tablas de rutas de VPC incluyen las tablas de rutas predeterminadas y personalizadas.

Notas y restricciones

Tabla 6-5 muestra los tipos de rutas que se pueden replicar.

Por ejemplo, si el salto siguiente de una ruta es un servidor, esta ruta se puede replicar en la tabla de rutas predeterminada o personalizada. Si el salto siguiente de una ruta es un gateway de Direct Connect, la ruta no se puede replicar en la tabla de rutas predeterminada, pero se puede replicar en una tabla de rutas personalizada.

Tabla 6-5 Descripción de replicación de ruta

Tipo del próximo salto	Replicado a la tabla de rutas por defecto	Replicado a la tabla de rutas personalizadas
Local	No se admite	No se admite
Server	Se admite	Se admite
Extension NIC	Se admite	Se admite
BMS user-defined network	No se admite	Se admite

Tipo del próximo salto	Replicado a la tabla de rutas por defecto	Replicado a la tabla de rutas personalizadas
VPN gateway	No se admite	Se admite
Direct Connect gateway	No se admite	Se admite
Cloud connection	No se admite	Se admite
Supplementary network interface	Se admite	Se admite
NAT gateway	Se admite	Se admite
VPC peering connection	Se admite	Se admite
Virtual IP address	Se admite	Se admite
Enterprise router	Se admite	Se admite
Cloud firewall	Se admite	Se admite

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, busque la fila que contiene la tabla de rutas de destino y haga clic en **Replicate Route** en la columna **Operation**.
6. Seleccione la tabla de ruta de destino y, a continuación, la ruta que se va a replicar según se le solicite.

   Las rutas que aparecen en la página son las que no existen en la tabla de rutas de destino. Puede seleccionar una o más rutas para replicar en la tabla de rutas de destino.
7. Haga clic en **OK**.

6.11 Eliminación de una ruta

Escenarios

Eliminar una ruta personalizada si ya no es necesaria.

Notas y restricciones

- No se puede eliminar la ruta del sistema.
- Las rutas entregadas por los servicios VPN, Direct Connect y Cloud Connect a la tabla de rutas predeterminada no se pueden eliminar.In addition, the route of a gateway VPC endpoint in the custom route table cannot be deleted.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tabla de rutas, haga clic en el nombre de la tabla de rutas de destino.
6. Busque la fila que contiene la ruta que se va a eliminar y haga clic en **Delete** en la columna **Operation**.
7. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

6.12 Configuración de un servidor SNAT

Scenarios

To use the route table function provided by the VPC service, you need to configure SNAT on an ECS to enable other ECSs that do not have EIPs bound in a VPC to access the Internet through this ECS.

The configured SNAT takes effect for all subnets in a VPC.

Prerequisites

- You have an ECS where SNAT is to be configured.
- The ECS where SNAT is to be configured runs the Linux OS.
- The ECS where SNAT is to be configured has only one network interface card (NIC).

Differences Between SNAT Servers and NAT Gateways

The NAT Gateway service provides network address translation (NAT) for servers, such as ECSs, BMSs and Workspace desktops, in a VPC or servers from an on-premises data center that connects to a VPC through Direct Connect or VPN. A NAT gateway allows these servers to share an EIP to access the Internet or provide services accessible from the Internet.

The NAT Gateway service is easier to configure and use than SNAT. This service can be flexibly deployed across subnets and AZs and provides different NAT gateway specifications. You can click **NAT Gateway** under **Networking** on the management console to try this service.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Compute**, haga clic en **Elastic Cloud Server**.
4. En la página mostrada, busque el ECS de destino en la lista de ECS y haga clic en el nombre de ECS para cambiar a la página que muestra los detalles de ECS.

5. En la página de detalles de ECS que se muestra, haga clic en la ficha **NICs**.
6. En el área mostrada que muestra los detalles de la dirección IP de la NIC, deshabilite la **Source/Destination Check**.

   De forma predeterminada, la comprobación de origen/destino está habilitada. Cuando esta comprobación está habilitada, el sistema comprueba si las direcciones IP de origen contenidas en los paquetes enviados por ECS son correctas. Si las direcciones IP son incorrectas, el sistema no permite que los ECS envíen los paquetes. Este mecanismo evita la suplantación de paquetes, mejorando así la seguridad del sistema. Si se utiliza la función de SNAT, el servidor de SNAT necesita reenviar paquetes. Este mecanismo impide que el remitente del paquete reciba paquetes devueltos. Por lo tanto, debe deshabilitar la comprobación de origen/destino para servidores de SNAT.
7. Vincular una EIP.
   - Vincula una EIP a la dirección IP privada del ECS.
   - Vincula una EIP a la dirección IP virtual del ECS.
8. En la consola de ECS, utilice la función de inicio de sesión remoto para iniciar sesión en ECS donde va a configurar SNAT.
9. Ejecute el siguiente comando e introduzca la contraseña de usuario **root** para cambiar a usuario **root**:

   su - root
10. Ejecute el siguiente comando para comprobar si el ECS puede conectarse correctamente a Internet:

    NOTA

    Antes de ejecutar el comando, debe deshabilitar la regla iptables de respuesta en el ECS donde está configurado SNAT y habilitar las reglas del grupo de seguridad.

    ping www.huawei.com

    El ECS puede acceder a Internet si se muestra la siguiente información:

    ```
    [root@localhost ~]# ping www.huawei.com
    PING www.a.shifen.com (xxx.xxx.xxx.xxx) 56(84) bytes of data.
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=51 time=9.34 ms
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=51 time=9.11 ms
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=51 time=8.99 ms
    ```
11. Ejecute el siguiente comando para comprobar si el reenvío IP del SO de Linux está habilitado:

    cat /proc/sys/net/ipv4/ip_forward

    En la salida del comando, **1** indica que está habilitado y **0** indica que está deshabilitado. El valor predeterminado es 0.
    - Si el reenvío de IP en Linux está habilitado, vaya al paso **14**.
    - Si el reenvío de IP en Linux está deshabilitado, vaya a **12** a habilitar el reenvío de IP en Linux.

    Muchos SO soportan el enrutamiento de paquetes. Antes de reenviar paquetes, los SO cambian las direcciones IP de origen en los paquetes a direcciones IP SO. Por lo tanto, los paquetes reenviados contienen la dirección IP del emisor público de modo que los paquetes de respuesta pueden enviarse de vuelta a lo largo de la misma ruta al emisor de paquetes inicial. Este método se llama SNAT. Los SO necesitan realizar un seguimiento de los paquetes en los que se han cambiado las direcciones IP para garantizar que las direcciones IP de destino en los paquetes se pueden reescribir y que los paquetes se pueden reenviar al emisor inicial del paquete. Para lograr estos fines, debe habilitar la función de reenvío de IP y configurar las reglas SNAT.

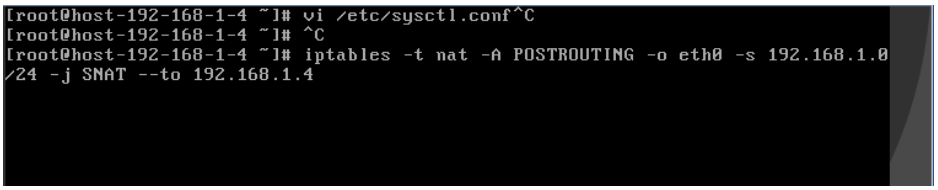
12. Utilice el editor vi para abrir el archivo **/etc/sysctl.conf**, cambie el valor de **net.ipv4.ip_forward** a **1**, e introduzca **:wq** para guardar el cambio y salir.
13. Ejecute el siguiente comando para hacer que el cambio surta efecto:

    sysctl -p /etc/sysctl.conf
14. Configure la función de SNAT.

    Ejecute el siguiente comando para habilitar todos los ECS de la red (por ejemplo, 192.168.1.0/24) para acceder a Internet mediante la función SNAT:

    iptables -t nat -A POSTROUTING -o eth0 -s subnet -j SNAT --to nat-instance-ip

Figura 6-4 Configuración de SNAT



NOTA

Para asegurarse de que la regla no se perderá después del reinicio, escriba la regla en el archivo **/etc/rc.local**.

1. Cambie al archivo **/etc/sysctl.conf**:

   vi /etc/rc.local
2. Realizar **14** para configurar SNAT.
3. Guarde la configuración y salga:

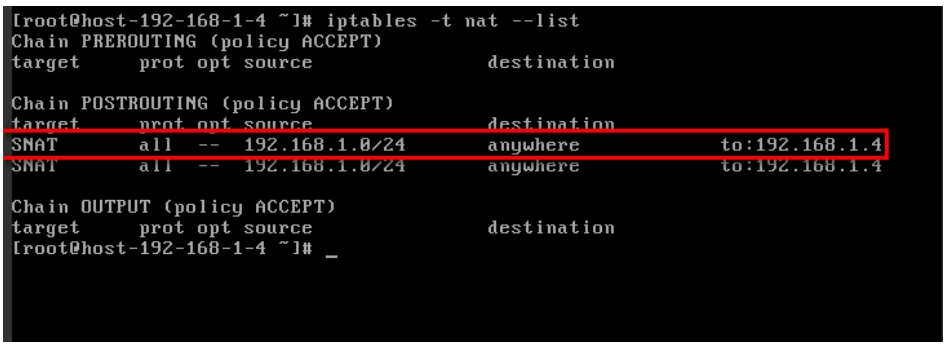
   :wq
4. Agregue los permisos de ejecución para el archivo **rc.local**:

   # chmod +x /etc/rc.local

15. Compruebe si la configuración se ha realizado correctamente. Si se muestra información similar a **Figura 6-5** (por ejemplo, 192.168.1.0/24), la configuración se ha realizado correctamente.

    iptables -t nat --list

Figura 6-5 Verificación de la configuración



16. Agregue una ruta. Para obtener más información, consulte la sección **Adición de una ruta personalizada**.

    Establezca el destino en **0.0.0.0/0**, y el salto siguiente a la dirección IP privada o virtual del ECS donde se implementa SNAT. Por ejemplo, el salto siguiente es **192.168.1.4**.

Una vez completadas estas operaciones, si la comunicación de red sigue fallando, compruebe la configuración del grupo de seguridad y de ACL de red para ver si se permite el tráfico requerido.

7 Interconexión de VPC

7.1 Descripción general de interconexión de VPC

Una interconexión de VPC es una conexión de red entre dos VPC en una región que le permite enrutar el tráfico entre ellos mediante las direcciones IP privadas. Los ECS en cualquiera de las VPC pueden comunicarse entre sí como si estuvieran en la misma región. Puede crear una interconexión de VPC entre sus propias VPC, o entre su VPC y la de otra cuenta dentro de la misma región. Sin embargo, no puede crear una interconexión de VPC entre las VPC en diferentes regiones.

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.

7.2 Planes de configuración de interconexión de VPC

Las VPC se aíslan entre sí. Para conectar dos VPC en la misma región, puede utilizar una interconexión de VPC para enrutar el tráfico entre ellos mediante direcciones IP privadas.

Estos son algunos escenarios que le ayudarán a determinar qué configuración se adapta mejor a sus requisitos de red.

Tabla 7-1 Casos de la interconexión de VPC

Caso	Descripción de la configuración
● Los bloques CIDR de VPC no se superponen. ● Los bloques CIDR de subred no se superponen.	Cree las interconexiones de VPC para conectar bloques CIDR completos de VPC.

Caso	Descripción de la configuración
● Los bloques CIDR de VPC se superponen. ● Algunos bloques CIDR de subred no se superponen.	Cree interconexión de VPC para conectar subredes específicas o ECS de diferentes VPC. ● Para conectar subredes específicas desde dos VPC, los bloques CIDR de subred no se pueden superponer. ● Para conectar los ECS específicos desde dos VPC, cada ECS debe tener una dirección IP privada única.
● Los bloques CIDR de VPC se superponen. ● Los bloques CIDR de subred se superponen.	Las interconexiones de VPC no son utilizables.

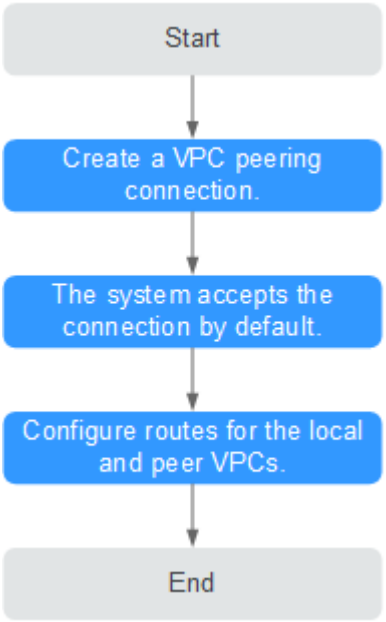
7.3 Creación de una interconexión de VPC con otra VPC en su cuenta.

Escenarios

Para crear una interconexión de VPC, primero cree una solicitud para conectar con otra VPC. Puede solicitar una interconexión de VPC con otra VPC en su cuenta, pero las dos VPC deben estar en la misma región. El sistema acepta la solicitud automáticamente.

Procedimiento

Figura 7-1 Creación de una interconexión de VPC entre las VPC de su cuenta



Si crea una interconexión de VPC entre dos VPC de su cuenta, el sistema acepta la conexión de forma predeterminada. Es necesario agregar rutas para las VPC locales y del mismo nivel para permitir la comunicación entre las dos VPC.

Prerrequisitos

Se han creado dos VPC en la misma región.

Creación de una interconexión de VPC

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
5. En el panel derecho que se muestra, haga clic en **Create VPC Peering Connection**.
6. Configure los parámetros según se le solicite. Debe seleccionar **My account** para **Account**. **Tabla 7-2** enumera los parámetros que se van a configurar.

Figura 7-2 Crear la interconexión de VPC

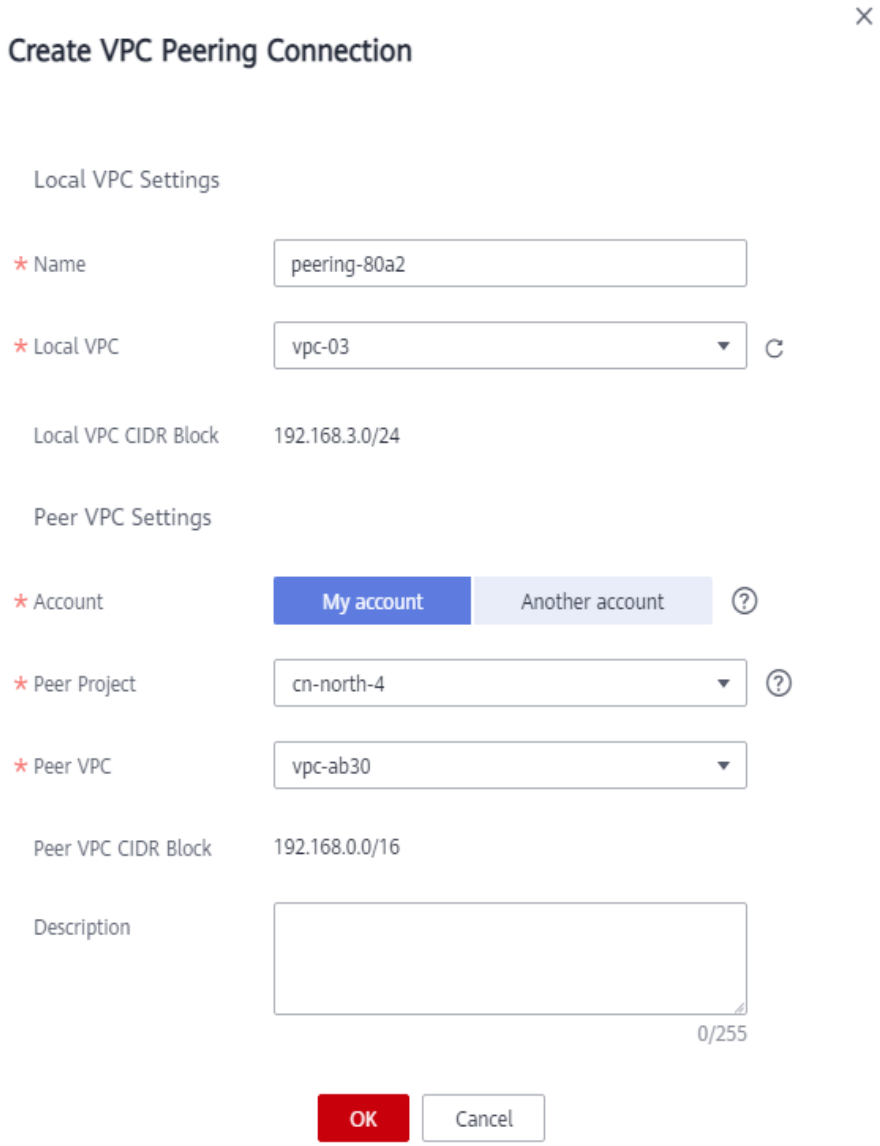


Tabla 7-2 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	El nombre de la interconexión de VPC. El nombre contiene un máximo de 64 caracteres, que consisten en letras, dígitos, guiones (-) y guiones bajos (_).	peering-001
Local VPC	La VPC local. Puede seleccionar uno de la lista desplegable.	vpc_01

Parámetro	Descripción	Valor de ejemplo
Local VPC CIDR Block	El bloque CIDR para la VPC local.	192.168.10.0/24
Account	La cuenta a la que pertenece la VPC del mismo nivel. ● **My account**: La interconexión de VPC se creará entre dos VPC, en la misma región, en su cuenta. ● **Another account**: La interconexión de VPC se creará entre su VPC y una VPC en otra cuenta, en la misma región.	My account
Peer Project	El nombre del proyecto del mismo nivel. El nombre del proyecto actual se utiliza de forma predeterminada.If you select the project name of a DeC, you can create a VPC peering connection with a VPC in a DeC that is in the same region as the local VPC.	aaa
Peer VPC	La VPC del mismo nivel. Puede seleccionar uno de la lista desplegable si la interconexión de VPC se crea entre dos VPC en su propia cuenta.	vpc_02
Peer VPC CIDR Block	El bloque CIDR para la VPC del mismo nivel. Las VPC locales y pares no pueden tener bloques CIDR coincidentes o superpuestos. De lo contrario, las rutas agregadas para la interconexión de VPC pueden no tener efecto.	192.168.2.0/24
Description	Información complementaria sobre la interconexión de VPC. Este parámetro es opcional. La descripción del interconexión de VPC puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. Haga clic en **OK**.

Adición de rutas para una interconexión de VPC

Si solicita una interconexión de VPC con otra VPC en su propia cuenta, el sistema acepta automáticamente la solicitud. Para habilitar la comunicación entre las dos VPC, debe agregar rutas locales y de pares en la página **Route Tables** para la interconexión de VPC.

1. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
2. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
3. Busque el interconexión de VPC para el que desea configurar las rutas en la lista de conexiones y haga clic en el nombre de la conexión.

   Se muestra la página que muestra los detalles del interconexión de VPC.
4. Agregue rutas para el interconexión de VPC a la tabla de rutas de la VPC local:
   a. Haga clic en la ficha **Local Routes** y, a continuación, haga clic en el hipervínculo **Route Tables**.

      Se muestra la ficha **Summary** de la tabla de ruta predeterminada para la VPC local.
   b. Haga clic en la ficha **Associated Subnets** para ver las subredes asociadas a la tabla de rutas predeterminada.
      - Si existe la subred que se va a conectar mediante la interconexión de VPC,
        1) Haga clic en la ficha **Summary** de la tabla de rutas y haga clic en **Add Route** para agregar una ruta a la tabla de rutas predeterminada.

           Tabla 7-3 describe los parámetros de ruta.
      - Si la subred que se va a conectar por la interconexión de VPC no está allí,
        1) Vuelva a la lista de VPC y cambie a la lista de subred de la VPC.
        2) Busque la fila que contiene la subred de destino que va a ser conectada por la interconexión de VPC y haga clic en el nombre de la tabla de rutas en la columna **Route Table**.

           Se muestra la ficha **Summary** de la tabla de rutas asociada a la subred.
        3) Haga clic en **Add Route** para agregar una ruta a la tabla de rutas.

           Tabla 7-3 describe los parámetros de ruta.

Tabla 7-3 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Destination	El bloque CIDR de VPC del mismo nivel, el bloque CIDR de subred o la dirección IP de ECS. Para más detalles, consulte **Planes de configuración de interconexión de VPC**.	192.168.1.0/24
Next Hop Type	El siguiente tipo de salto. Seleccione **VPC peering connection**.	VPC peering connection
Next Hop	La dirección del salto siguiente. Seleccione el nombre de la interconexión de VPC actual.	peering-001

Parámetro	Descripción	Valor de ejemplo
Description	Información complementaria sobre la ruta. Este parámetro es opcional. La descripción de la ruta puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

5. Agregue rutas para el interconexión de VPC a la tabla de rutas de la VPC del mismo nivel:
   a. Haga clic en la ficha **Peer Routes** y, a continuación, haga clic en el hipervínculo **Route Tables**.
      Se muestra la ficha **Summary** de la tabla de ruta predeterminada para la VPC del mismo nivel.
   b. Haga clic en la ficha **Associated Subnets** para ver las subredes asociadas a la tabla de rutas predeterminada.
      - Si existe la subred que se va a conectar mediante la interconexión de VPC,
        1) Haga clic en la ficha **Summary** de la tabla de rutas y haga clic en **Add Route** para agregar una ruta a la tabla de rutas predeterminada.
           Tabla 7-4 describe los parámetros de ruta.
        2) Haga clic en **OK**.
      - Si la subred que se va a conectar por la interconexión de VPC no está allí,
        1) Vuelva a la lista de VPC y cambie a la lista de subred de la VPC.
        2) Busque la fila que contiene la subred de destino que va a ser conectada por la interconexión de VPC y haga clic en el nombre de la tabla de rutas en la columna **Route Table**.
           Se muestra la ficha **Summary** de la tabla de rutas asociada a la subred.
        3) Haga clic en **Add Route** para agregar una ruta a la tabla de rutas.
           Tabla 7-4 describe los parámetros de ruta.
        4) Haga clic en **OK**.

Tabla 7-4 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Destination	El bloque CIDR de VPC local, el bloque CIDR de subred o la dirección IP de ECS. Para más detalles, consulte **Planes de configuración de interconexión de VPC**.	192.168.3.0/24
Next Hop Type	El siguiente tipo de salto. Seleccione **VPC peering connection**.	VPC peering connection

Parámetro	Descripción	Valor de ejemplo
Next Hop	La dirección del salto siguiente. Seleccione el nombre de la interconexión de VPC actual.	peering-001
Description	Información complementaria sobre la ruta. Este parámetro es opcional. La descripción de la ruta puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

Después de crear una interconexión de VPC, las dos VPC pueden comunicarse entre sí a través de direcciones IP privadas. Puede ejecutar el comando **ping** para comprobar si las dos VPC pueden comunicarse entre sí. Antes de ejecutar el comando **ping**, asegúrese de que el grupo de seguridad permita el tráfico ICMP entrante. Para más detalles, consulte **Adición de una regla de grupo de seguridad**.

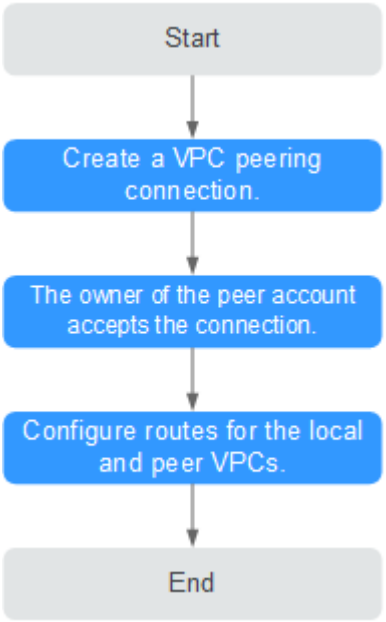
7.4 Creación de una interconexión de VPC con una VPC de otra cuenta

Escenarios

El servicio de VPC también le permite crear una interconexión de VPC con una VPC en otra cuenta. Las dos VPC deben estar en la misma región. Si solicita una interconexión de VPC con una VPC en otra cuenta de la misma región, el propietario de la cuenta de igual debe aceptar la solicitud para activar la conexión. Este servicio es gratuito y su cuenta y la cuenta de pares no se cobrará por esto.

Procedimiento

Figura 7-3 Creación de una interconexión de VPC con una VPC de otra cuenta



Si crea una interconexión de VPC entre su VPC y una VPC que está en otra cuenta, la interconexión de VPC estará en el estado **Awaiting acceptance**. Después de que el propietario de la cuenta del mismo nivel acepte la conexión, el estado de la conexión cambia a **Accepted**. Los propietarios de las cuentas local y del par deben configurar las rutas requeridas por la interconexión de VPC para permitir la comunicación entre las dos VPC.

Creación de una interconexión de VPC

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
5. En el panel derecho que se muestra, haga clic en **Create VPC Peering Connection**.
6. Configure los parámetros según se le solicite. Debe seleccionar **Another account** para **Account**.

Figura 7-4 Creación de una interconexión de VPC

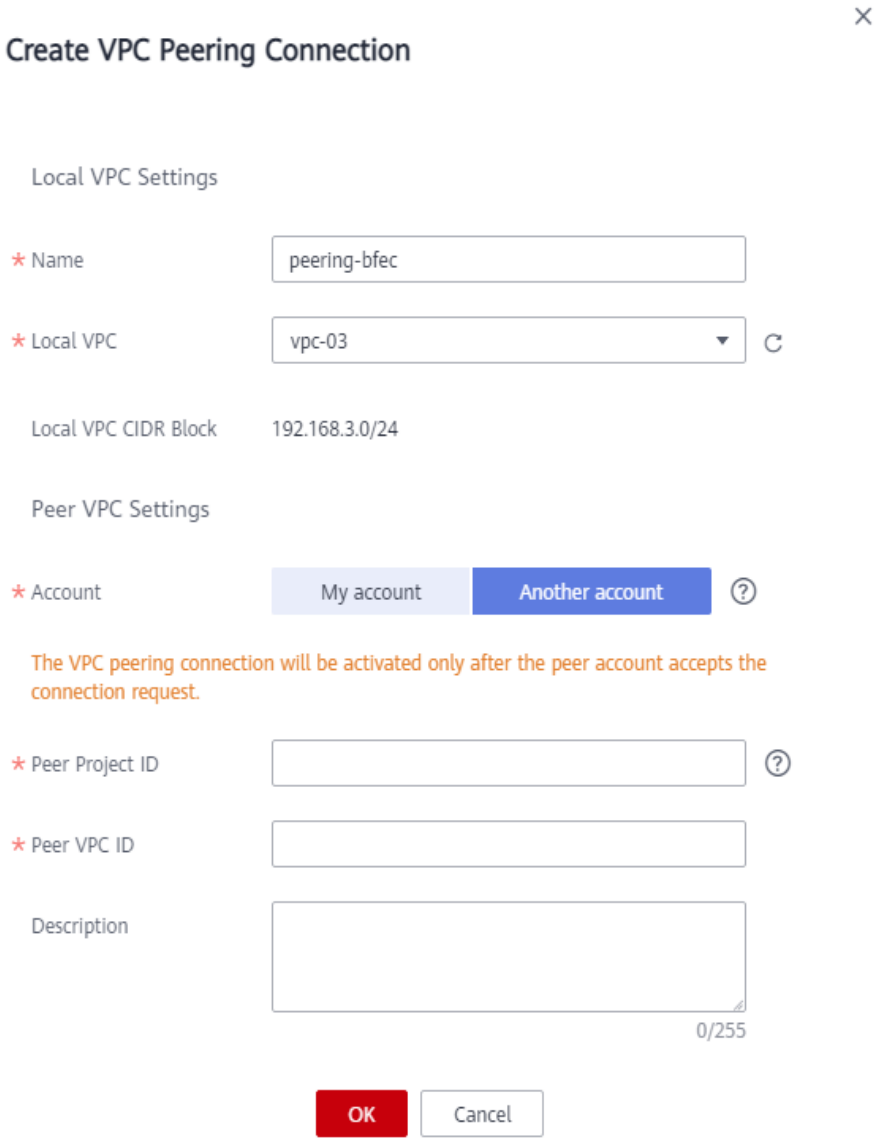


Tabla 7-5 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	El nombre de la interconexión de VPC. El nombre contiene un máximo de 64 caracteres, que consisten en letras, dígitos, guiones (-) y guiones bajos (_).	peering-002
Local VPC	La VPC local. Puede seleccionar uno de la lista desplegable.	vpc_01

Parámetro	Descripción	Valor de ejemplo
Account	La cuenta a la que pertenece la VPC al igualar. ● **My account**: La interconexión de VPC se creará entre dos VPC, en la misma región, en su cuenta. ● **Another account**: La interconexión de VPC se creará entre su VPC y una VPC en otra cuenta, en la misma región.	Another account
Peer Project ID	Este parámetro sólo está disponible cuando se selecciona **Another account**.	N/A
Peer VPC ID	Este parámetro sólo está disponible cuando se selecciona **Another account**.	65d062b3-40fa-4204-8181-3538f527d2ab
Description	Información complementaria sobre la interconexión de VPC. Este parámetro es opcional. La descripción del interconexión de VPC puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

7. Haga clic en **OK**.

NOTA

Si se muestra un mensaje que indica que se debe introducir el ID de VPC y el ID de proyecto correctos, es posible que la interconexión de VPC no se cree porque las VPC no están en la misma región. Puede utilizar Cloud Connect para habilitar la comunicación entre VPC en diferentes regiones.

Aceptación de una solicitud de interconexión de VPC

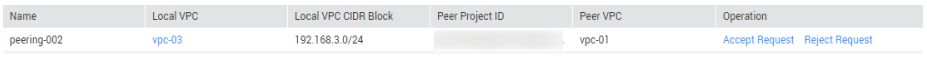
Para solicitar una interconexión de VPC con una VPC en otra cuenta, el propietario de la cuenta de igual debe aceptar la solicitud para activar la conexión.

NOTA

Para garantizar la seguridad, no acepte la interconexión de VPC de las cuentas desconocidas.

1. El propietario de la cuenta del par inicia 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 **VPC Peering**.
4. En la lista de solicitudes que se deben tramitar, busque la fila que contiene el interconexión de VPC de destino y haga clic en **Accept Request** en la columna **Operation**.

Figura 7-5 Lista de solicitudes que deben tramitarse



5. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Rechazar una interconexión de VPC

El propietario de la cuenta del par puede rechazar cualquier solicitud de interconexión de VPC que reciba. Si se rechaza una solicitud de interconexión de VPC, no se establecerá la conexión. Debe eliminar la solicitud de interconexión de VPC rechazada antes de crear una interconexión de VPC entre las mismas VPC que las de la solicitud rechazada.

1. El propietario de la cuenta del par inicia 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 **VPC Peering**.
4. En la lista de solicitudes que se deben tramitar, busque la fila que contiene el interconexión de VPC de destino y haga clic en **Reject Request** en la columna **Operation**.
5. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

Adición de rutas para una interconexión de VPC

Si solicita un interconexión de VPC con una VPC en otra cuenta, el propietario de la cuenta de igual debe aceptar la solicitud. Para habilitar la comunicación entre las dos VPC, los propietarios de las cuentas locales y de pares deben agregar rutas en la página **Route Tables** para la interconexión de VPC. El propietario de la cuenta local solo puede agregar la ruta local porque el propietario no tiene el permiso necesario para realizar operaciones en la VPC del mismo nivel. El propietario de la cuenta del par debe agregar la ruta del par. El procedimiento para agregar una ruta local y una ruta de pares es el mismo.

1. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
2. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
3. Busque el interconexión de VPC para el que desea configurar las rutas en la lista de conexiones y haga clic en el nombre de la conexión.

   Se muestra la página que muestra los detalles del interconexión de VPC.
4. Agregue rutas para el interconexión de VPC a la tabla de rutas de la VPC local:
   a. Haga clic en la ficha **Local Routes** y, a continuación, haga clic en el hipervínculo **Route Tables**.

      Se muestra la ficha **Summary** de la tabla de ruta predeterminada para la VPC local.
   b. Haga clic en la ficha **Associated Subnets** para ver las subredes asociadas a la tabla de rutas predeterminada.
      - Si existe la subred que se va a conectar mediante la interconexión de VPC,
        1) Haga clic en la ficha **Summary** de la tabla de rutas y haga clic en **Add Route** para agregar una ruta a la tabla de rutas predeterminada.

           Tabla 7-6 describe los parámetros de ruta.
      - Si la subred que se va a conectar por la interconexión de VPC no está allí,

1) Vuelva a la lista de VPC y cambie a la lista de subred de la VPC.
2) Busque la fila que contiene la subred de destino que va a ser conectada por la interconexión de VPC y haga clic en el nombre de la tabla de rutas en la columna **Route Table**.

   Se muestra la ficha **Summary** de la tabla de rutas asociada a la subred.
3) Haga clic en **Add Route** para agregar una ruta a la tabla de rutas.

   Tabla 7-6 describe los parámetros de ruta.

Tabla 7-6 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Destino	El bloque CIDR de VPC del mismo nivel, el bloque CIDR de subred o la dirección IP de ECS. Para más detalles, consulte **Planes de configuración de interconexión de VPC**.	192.168.1.0/24
Tipo del próximo salto	El siguiente tipo de salto. Seleccione **VPC peering connection**.	Interconexión de VPC
Próximo salto	La dirección del salto siguiente. Seleccione el nombre de la interconexión de VPC actual.	peering-001
Descripción	Información complementaria sobre la ruta. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

5. Agregue rutas para el interconexión de VPC a la tabla de rutas de la VPC del mismo nivel:
   a. Haga clic en la ficha **Peer Routes** y, a continuación, haga clic en el hipervínculo **Route Tables**.

      Se muestra la ficha **Summary** de la tabla de ruta predeterminada para la VPC del mismo nivel.
   b. Haga clic en la ficha **Associated Subnets** para ver las subredes asociadas a la tabla de rutas predeterminada.
      - Si existe la subred que se va a conectar mediante la interconexión de VPC,
        1) Haga clic en la ficha **Summary** de la tabla de rutas y haga clic en **Add Route** para agregar una ruta a la tabla de rutas predeterminada.

           Tabla 7-7 describe los parámetros de ruta.
        2) Haga clic en **OK**.
      - Si la subred que se va a conectar por la interconexión de VPC no está allí,
        1) Vuelva a la lista de VPC y cambie a la lista de subred de la VPC.

2) Busque la fila que contiene la subred de destino que va a ser conectada por la interconexión de VPC y haga clic en el nombre de la tabla de rutas en la columna **Route Table**.

   Se muestra la ficha **Summary** de la tabla de rutas asociada a la subred.

3) Haga clic en **Add Route** para agregar una ruta a la tabla de rutas.

   Tabla 7-7 describe los parámetros de ruta.

4) Haga clic en **OK**.

Tabla 7-7 Descripción del parámetro

Parámetro	Descripción	Valor de ejemplo
Destino	El bloque CIDR de VPC local, el bloque CIDR de subred o la dirección IP de ECS. Para más detalles, consulte **Planes de configuración de interconexión de VPC**.	192.168.3.0/24
Next Hop Type	El siguiente tipo de salto. Seleccione **VPC peering connection**.	VPC peering connection
Next Hop	La dirección del salto siguiente. Seleccione el nombre de la interconexión de VPC actual.	peering-001
Description	Información complementaria sobre la ruta. Este parámetro es opcional. La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	-

Después de crear una interconexión de VPC, las dos VPC pueden comunicarse entre sí a través de direcciones IP privadas. Puede ejecutar el comando **ping** para comprobar si las dos VPC pueden comunicarse entre sí. Antes de ejecutar el comando **ping**, asegúrese de que el grupo de seguridad permita el tráfico ICMP entrante. Para más detalles, consulte **Adición de una regla de grupo de seguridad**.

Obtención del ID del proyecto de pares

1. El propietario de la cuenta del par inicia sesión en la consola de gestión.
2. Seleccione **My Credentials** en la lista desplegable nombre de usuario.
3. En la ficha **Projects**, obtenga el ID de proyecto requerido.

Obtención del ID de VPC del mismo nivel

1. El propietario de la cuenta del par inicia 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. Haga clic en el nombre de la VPC de destino y vea el ID de la VPC en la página de detalles de la VPC.

7.5 Modificación de una interconexión de VPC

Escenarios

Los propietarios de las cuentas locales y de pares pueden modificar una interconexión de VPC en cualquier estado. El nombre de la interconexión de VPC se puede cambiar.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
5. En el panel que se muestra a la derecha, vea información sobre las interconexión de VPC. Puede buscar las interconexiones de VPC específicas por estado de conexión o por nombre.
6. Busque el interconexión de VPC de destino y haga clic en **Modify** en la columna **Operation**. En el cuadro de diálogo que se muestra, modifique la información sobre el interconexión de VPC.
7. Haga clic en **OK**.

7.6 Consulta de interconexiones de VPC

Escenarios

Los propietarios de las cuentas locales y de pares pueden ver información sobre las interconexión de VPC creadas y aquellas que todavía están esperando a ser aceptadas.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
5. En el panel que se muestra a la derecha, vea información sobre las interconexión de VPC. Puede buscar las interconexiones de VPC específicas por estado de conexión o por nombre.
6. Haga clic en el nombre de la interconexión de VPC. En la página mostrada, vea la información detallada sobre la interconexión de VPC.

7.7 Eliminación de una interconexión de VPC

Escenarios

Los propietarios de las cuentas locales y de pares pueden eliminar una interconexión de VPC en cualquier estado. Después de eliminar una interconexión de VPC, las rutas configuradas para la conexión también se eliminarán automáticamente.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
5. En el panel que se muestra a la derecha, vea información sobre las interconexión de VPC. Puede buscar las interconexiones de VPC específicas por estado de conexión o por nombre.
6. Busque el interconexión de VPC de destino y haga clic en **Delete** en la columna **Operation**.
7. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

7.8 Consulta de rutas configuradas para una interconexión de VPC

Escenarios

Después de agregar rutas para una interconexión de VPC, los propietarios de las cuentas locales y de pares pueden ver información sobre las rutas en la página que muestra detalles sobre la interconexión de VPC.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
5. Busque la interconexión de VPC de destino en la lista de conexiones.
6. Haga clic en el nombre de la interconexión de VPC para cambiar a la página que muestra detalles sobre la conexión.

7. En la página mostrada, haga clic en la ficha **Local Routes** y vea información sobre la ruta local agregada para la interconexión de VPC.
8. En la página que muestra los detalles sobre la interconexión de VPC, haga clic en la ficha **Peer Routes** y vea información sobre la ruta de pares agregada para la interconexión de VPC.

NOTA

Si ha establecido una interconexión de VPC pero las dos VPC no pueden comunicarse entre sí, realice los pasos anteriores para comprobar si las rutas local y peer están correctamente configuradas.

7.9 Eliminación de una interconexión de VPC

Escenarios

Después de agregar las rutas para un interconexión de VPC, los propietarios de las cuentas local y de pares pueden eliminar las rutas en la página que muestra detalles sobre el interconexión o en la página **Route Tables**.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **VPC Peering**.
5. En la lista de conexiones, busque la interconexión de VPC que necesita para eliminar las rutas.
6. Haga clic en el nombre de la interconexión de VPC para cambiar a la página que muestra detalles sobre la conexión.
7. Eliminar la ruta agregada a la tabla de rutas de la VPC local:
   a. Haga clic en la ficha **Local Routes** y, a continuación, haga clic en el hipervínculo **Route Tables**.

      Se muestra la ficha **Summary** de la tabla de ruta predeterminada para la VPC local.
   b. Busque la fila que contiene la ruta que se va a eliminar y haga clic en **Delete** en la columna **Operation**.
   c. Haga clic en **Yes**.
8. Elimine la ruta agregada a la tabla de rutas de la VPC del mismo nivel:
   a. Haga clic en la ficha **Peer Routes** y, a continuación, haga clic en el hipervínculo **Route Tables**.

      Se muestra la ficha **Summary** de la tabla de ruta predeterminada para la VPC del mismo nivel.
   b. Busque la fila que contiene la ruta que se va a eliminar y haga clic en **Delete** en la columna **Operation**.
   c. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

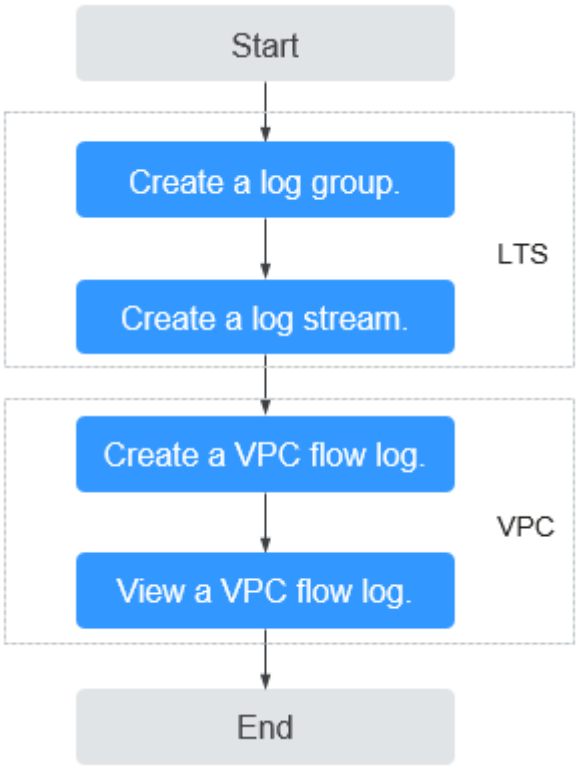
8 Log de flujo de VPC

8.1 Descripción general del log de flujo de VPC

Un log de flujo de VPC registra información sobre el tráfico que va hacia y desde una VPC. Logs de flujo de VPC le ayudan a supervisar el tráfico de red, analizar los ataques de red y determinar si los grupos de seguridad y las reglas de ACL de red requieren modificaciones.

Logs de flujo de VPC deben usarse junto con el Log Tank Service (LTS). Antes de crear un log de flujo de VPC, debe crear un grupo de log y un flujo de log en LTS. **Figura 8-1** muestra el proceso para configurar la función de log de flujo de VPC.

Figura 8-1 Configuración de la función de log de flujo de VPC



La función de log de flujo de VPC en sí es gratuita, pero se le puede cobrar por otros recursos utilizados. Por ejemplo, se cobrará el almacenamiento de logs de flujo de VPC. Para obtener más información, consulte la Guía del usuario de Log Tank Service.

Notas y restricciones

- Actualmente, solo los ECS S2, M2, Hc2, D2, Pi1, S3, C3, M3, H3, Ir3, I3, S6, E3, C3ne, M3ne, G5, P2v, C6, M6, Pi1, y H3 admiten logs de flujo de VPC.
- De forma predeterminada, puede crear un máximo de 10 logs de flujo de VPC.
- De forma predeterminada, se admite un máximo de 400,000 logs de flujo.

8.2 Creación de un log de flujo de VPC

Escenarios

Un log de flujo de VPC registra información sobre el tráfico que va hacia y desde una VPC.

Prerrequisitos

Asegúrese de que se han realizado las siguientes operaciones en la consola de LTS:

- Cree un grupo de log.
- Crear un flujo de log.

Para obtener más información acerca del servicio LTS, consulte la *Guía del usuario de Log Tank Service*.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **VPC Flow Logs**.
5. En la esquina superior derecha, haga clic en **Create VPC Flow Log**. En la página mostrada, configure los parámetros según se le solicite.

Tabla 8-1 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	El nombre del log de flujo de VPC. El nombre puede contener un máximo de 64 caracteres, que pueden consistir en letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). El nombre no puede contener espacios.	flowlog-495d

Parámetro	Descripción	Valor de ejemplo
Resource Type	El tipo de recursos cuyo tráfico se va a registrar. Puede seleccionar **NIC**, **Subnet**, o **VPC**.	NIC
Resource	La NIC específica cuyo tráfico se va a registrar. **NOTA** Le recomendamos que seleccione un ECS que esté en el estado de ejecución. Si se selecciona un ECS en el estado detenido, reinicie el ECS después de crear el log de flujo de VPC para registrar con precisión la información sobre el tráfico que va hacia y desde la NIC de ECS.	N/A
Filter	● **All traffic**: especifica que se registrará tanto el tráfico aceptado como el rechazado del recurso especificado. ● **Accepted traffic**: especifica que solo se registrará el tráfico aceptado del recurso especificado. El tráfico aceptado se refiere al tráfico permitido por el grupo de seguridad o ACL de red. ● **Rejected traffic**: especifica que solo se registrará el tráfico rechazado del recurso especificado. El tráfico rechazado se refiere al tráfico denegado por el ACL de red.	All
Log Group	El grupo de log creado en LTS.	lts-group-wule
Log Stream	El flujo de log creado en LTS.	lts-topic-wule
Description	Información complementaria sobre el log de flujo de VPC. Este parámetro es opcional. La descripción del log de flujo de VPC puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	N/A

NOTA

Solo se pueden crear dos logs de flujo, cada uno con un filtro diferente, para un solo recurso bajo el mismo grupo de logs y el mismo flujo de log. Cada log de flujo de VPC debe ser único.

6. Haga clic en **OK**.

8.3 Consulta de un log de flujo de VPC

Escenarios

Ver información acerca de su log de flujo.

La ventana de captura es de aproximadamente 10 minutos, lo que indica que se generará un log de flujo cada 10 minutos. Después de crear un log de flujo de VPC, debe esperar unos 10 minutos antes de poder ver el log de flujo.

NOTA

Si un ECS está en el estado detenido, no se mostrarán sus registros de log de flujo.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **VPC Flow Logs**.
5. Busque el log de flujo de VPC de destino y haga clic en **View Log Record** en la columna **Operation** para ver información sobre el log de flujo en LTS.

   El registro de log de flujo tiene el siguiente formato:

   ```
   <version> <project-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport>
   <protocol> <packets> <bytes> <start> <end> <action> <log-status>
   ```

   Ejemplo 1: El siguiente es un ejemplo de un registro de log de flujo en el que se registraron datos durante la ventana de captura:

   ```
   1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd
   192.168.0.154 192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACCEPT OK
   ```

   El valor **1** indica la versión del log de flujo de VPC. Tráfico con un tamaño de 96 bytes a NIC **1d515d18-1b36-47dc-a983-bd6512aed4bd** durante los últimos 10 minutos (de 16:55:36 a 17:05:36 el 29 de enero, 2019) fue permitido. Se transmitió un paquete de datos a través del protocolo UDP desde la dirección IP de origen **192.168.0.154** y el puerto **38929** a la dirección IP de destino **192.168.3.25** y el puerto **53**.

   Ejemplo 2: El siguiente es un ejemplo de un registro de log de flujo en el que no se registraron datos durante la ventana de captura:

   ```
   1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - -
   - - - - 1431280876 1431280934 - NODATA
   ```

   Ejemplo 3: A continuación se muestra un ejemplo de un registro de log de flujo en el que se omitieron datos durante la ventana de captura:

   ```
   1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - -
   - - - - 1431280876 1431280934 - SKIPDATA
   ```

   Tabla 8-2 describe los campos de un registro de log de flujo.

Tabla 8-2 Descripción del campo de registro

Campo	Descripción	Valor de ejemplo
version	La versión del log de flujo de VPC.	1
project-id	El ID del proyecto.	5f67944957444bd6bb4fe3b367de8f3d

Campo	Descripción	Valor de ejemplo
interface-id	El ID de la NIC para la que se registra el tráfico.	1d515d18-1b36-47dc-a983-bd6512aed4bd
srcaddr	La dirección IP de origen.	192.168.0.154
dstaddr	La dirección IP de destino.	192.168.3.25
srcport	El puerto de origen.	38929
dstport	El puerto de destino.	53
protocol	El número de protocolo de la Autoridad de Números Asignados de Internet (IANA) del tráfico.	17
packets	Número de paquetes transferidos durante la ventana de captura.	1
bytes	Número de bytes transferidos durante la ventana de captura.	96
start	El tiempo, en segundos Unix, del inicio de la ventana de captura.	1548752136
end	El tiempo, en segundos Unix, del final de la ventana de captura.	1548752736
action	La acción asociada con el tráfico: ● **ACCEPT**: El tráfico registrado fue permitido por los grupos de seguridad o ACL de red. ● **REJECT**: El tráfico registrado fue denegado por los ACL de red.	ACCEPT

Campo	Descripción	Valor de ejemplo
log-status	El estado de registro del log de flujo de VPC: ● **OK**: Los datos se registran normalmente en los destinos elegidos. ● **NODATA**: No hubo tráfico de la configuración del **Filter** hacia o desde la NIC durante la ventana de captura. ● **SKIPDATA**: Algunos registros de log de flujo se omitieron durante la ventana de captura. Esto puede ser causado por una restricción de capacidad interna o un error interno. Por ejemplo: Cuando **Filter** se establece en **Accepted traffic**, si hay tráfico aceptado, el valor de **log-status** es **OK**. Si no hay tráfico aceptado, el valor de **log-status** es **NODATA** independientemente de si hay tráfico rechazado. Si algún tráfico aceptado se omite de forma anormal, el valor de **log-status** es **SKIPDATA**.	OK

Puede introducir una palabra clave en la página de detalles de flujo del log en la consola de LTS para buscar logs de flujo.

8.4 Habilitación o deshabilitación de log de flujo de VPC

Escenarios

Después de crear un log de flujo de VPC, el log de flujo de VPC se habilita automáticamente. Si no necesita registrar datos de tráfico, puede deshabilitar el log de flujo de VPC correspondiente. El log de flujo de VPC deshabilitado se puede activar de nuevo.

Procedimiento

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

3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **VPC Flow Logs**.
5. Busque el log de flujo de VPC que desea **Enable** o **Disable** y haga clic en Habilitar o Deshabilitar en la columna **Operation**.
6. Haga clic en **Yes**.

8.5 Eliminación de un log de flujo de VPC

Escenarios

Eliminar un log de flujo de VPC que no sea necesario. La eliminación de un log de flujo de VPC no eliminará los registros de log de flujo existentes en LTS.

NOTA

Si se elimina una NIC que utiliza un log de flujo de VPC, el log de flujo se eliminará automáticamente. Sin embargo, los registro de log de flujo no se eliminan.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **VPC Flow Logs**.
5. Busque la fila que contiene el log de flujo de VPC que se va a eliminar y haga clic en **Delete** en la columna **Operation**.
6. Haga clic en **Yes** en el cuadro de diálogo que aparece en pantalla.

9 Dirección IP virtual

9.1 Descripción general de la dirección IP virtual

¿Qué es una dirección IP virtual?

Una dirección IP virtual se puede compartir entre múltiples ECS. Un ECS puede tener direcciones IP privadas y virtuales, y puede acceder al ECS a través de cualquiera de las direcciones IP. Una dirección IP virtual tiene las mismas capacidades de acceso a la red que una dirección IP privada, incluida la comunicación de capa 2 y capa 3 en VPC, el acceso entre VPC mediante las interconexiones de VPC, así como el acceso a través de las EIP, las conexiones de VPN y las conexiones de Direct Connect.

Puede vincular ECS implementados en modo activo/en standby con la misma dirección IP virtual y, a continuación, vincular una EIP a la dirección IP virtual. Las direcciones IP virtuales pueden trabajar junto con Keepalived para garantizar una alta disponibilidad y recuperación ante desastres. Si el ECS activo es defectuoso, el ECS en standby toma automáticamente los servicios del activo.

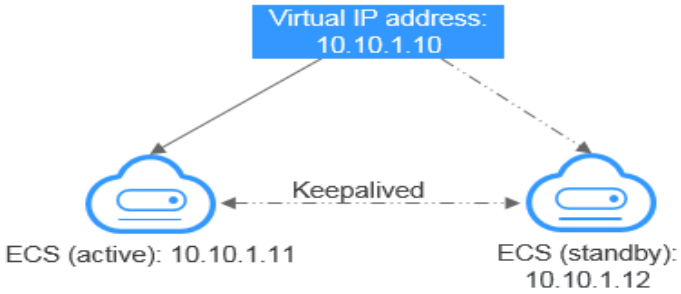
Redes

Las direcciones IP virtuales se utilizan para una alta disponibilidad y pueden trabajar junto con Keepalived para hacer posible la conmutación activa/en standby del ECS. De esta manera, si un ECS se cae por alguna razón, el otro puede hacerse cargo y los servicios continúan ininterrumpidos. Los ECS se pueden configurar para HA o como clústeres de equilibrio de carga.

- **Modo de la red 1**: HA

  Si desea mejorar la disponibilidad del servicio y evitar puntos únicos de error, puede implementar los ECS en el modo activo/en standby o implementar un ECS activo y varios ECS en standby. En esta disposición, todos los ECS usan la misma dirección IP virtual. Si el ECS activo se vuelve defectuoso, un ECS en standby se hace cargo de los servicios del ECS activo y los servicios continúan sin interrupciones.

Figura 9-1 Diagrama de red del modo de HA

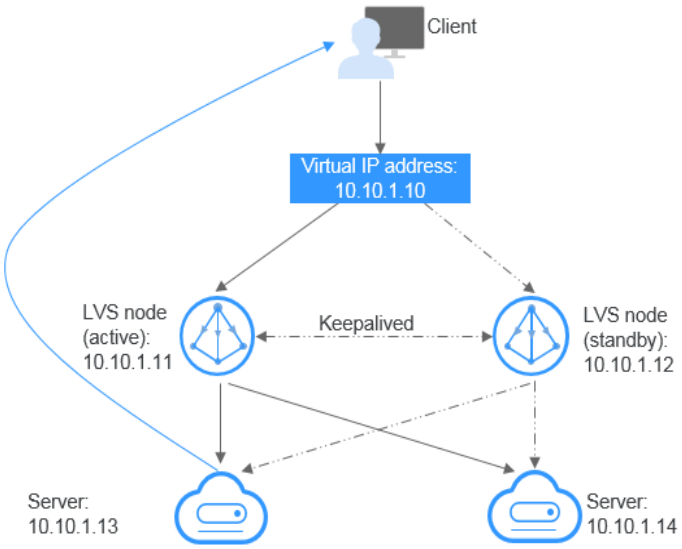


- En esta configuración, una única dirección IP virtual está vinculada a dos ECS en la misma subred.
- A continuación, Keepalived se utiliza para configurar los dos ECS para que funcionen en el modo activo/en standby. Siga los estándares de la industria para configurar Keepalived. Los detalles no están incluidos aquí.

- **Networking mode 2**: clúster de equilibrio de carga HA

  Si desea crear un clúster de equilibrio de carga de alta disponibilidad, utilice Keepalived y configure los nodos de LVS como los router directos.

Figura 9-2 clúster de equilibrio de carga de HA



- Vincule una única dirección IP virtual a dos ECS.
- Configure los dos ECS como nodos de LVS que funcionan como enrutadores directos y use Keepalived para configurar los nodos en el modo activo/en standby. Los dos ECS reenviarán uniformemente las solicitudes a diferentes servidores backend.
- Configure dos ECS más como servidores de backend.
- Deshabilite la comprobación de origen/destino de los dos servidores backend.
- Compruebe si la comprobación de origen/destino está deshabilitada en los ECS LVS activo y en standby. Para más detalles, consulte **Desactivación de la**

comprobación de origen y destino (escenario de clúster de equilibrio de carga HA).

Si vincula un ECS a una dirección IP virtual en la consola de gestión, la comprobación de origen/destino se deshabilita automáticamente. Si vincula un ECS a una dirección IP virtual llamando a las API, debe deshabilitar manualmente la comprobación de origen/destino.

Siga los estándares de la industria para configurar Keepalived. Los detalles no están incluidos aquí.

Notas y restricciones

- Las direcciones IP virtuales no se recomiendan cuando se configuran varias NIC en la misma subred en un ECS. Es demasiado fácil que haya conflictos de ruta en el ECS, lo que causaría un fallo de comunicación usando la dirección IP virtual.
- Una dirección IP virtual solo puede enlazarse a ECS en la misma subred.
- El reenvío IP debe estar deshabilitado en el ECS en standby. Para más detalles, consulte **Desactivación del reenvío de IP en el ECS en espera**.
- Cada dirección IP virtual puede estar vinculada a una sola EIP.
- Un ECS puede tener hasta ocho direcciones IP virtuales enlazadas.
- Una dirección IP virtual puede estar vinculada a hasta 10 ECS.
- Las direcciones IP virtuales y las NIC de extensión no se pueden utilizar para acceder directamente a los servicios de Huawei Cloud, como DNS. Puede utilizar VPCEP para acceder a estos servicios.

9.2 Asignación de una dirección IP virtual

Escenarios

Si un ECS requiere una dirección IP virtual o si es necesario reservar una dirección IP virtual, puede asignar una dirección IP virtual desde la subred.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Subnets**.
5. En la lista de subred, haga clic en el nombre de la subred a la que se va a asignar una dirección IP virtual.
6. Haga clic en la ficha **IP Addresses** y haga clic en **Assign Virtual IP Address**.
7. Seleccione un modo de asignación de direcciones IP virtuales.
   - **Automatic**: El sistema asigna una dirección IP automáticamente.
   - **Manual**: Puede especificar una dirección IP.
8. Seleccione **Manual** e introduzca una dirección IP virtual.

9. Haga clic en **OK**.

A continuación, puede consultar la dirección IP virtual asignada en la lista de direcciones IP.

9.3 Vinculación de una dirección IP virtual a una EIP o un ECS

Escenarios

Puede vincular una dirección IP virtual a una EIP para que pueda acceder a los ECS vinculados con la misma dirección IP virtual desde Internet. Estos ECS pueden trabajar en el modo activo/en standby para mejorar la tolerancia a fallos.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Subnets**.
5. En la lista de subred, haga clic en el nombre de la subred a la que pertenece la dirección IP virtual.
6. Haga clic en la ficha **IP Addresses**, busque la fila que contiene la dirección IP virtual de destino y haga clic en **Bind to EIP** o **Bind to Server** en la columna **Operation**.
7. Seleccione la EIP deseada o el ECS y su NIC.

   NOTA

   - Si el ECS tiene varias NIC, vincule la dirección IP virtual a la NIC principal.
   - Se pueden enlazar varias direcciones IP virtuales a una NIC de ECS.
8. Haga clic en **OK**.
9. Configure manualmente la dirección IP virtual vinculada a un ECS.

   Una vez que una dirección IP virtual está vinculada a una NIC de ECS, debe configurar manualmente la dirección IP virtual en el ECS.

   Linux OS (CentOS 7.2 64bit se usa como ejemplo.)

   a. Ejecute el siguiente comando para obtener la NIC a la que se debe vincular la dirección IP virtual y la conexión de la NIC:

      nmcli connection

      La información que aparecerá en pantalla será similar a la información siguiente:

      El resultado del comando en este ejemplo se describe de la siguiente manera:

      - **eth0** en la columna **DEVICE** indica la NIC a la que se debe vincular la dirección IP virtual.

- **Wired connection 1** en la columna **NAME** indica la conexión de la NIC.

b. Ejecute el siguiente comando para agregar la dirección IP virtual para la conexión de destino:

nmcli connection modify "*CONNECTION***" ipv4.addresses** *VIP*

Configure los parámetros de la siguiente manera:

- CONNECTION: conexión de la NIC obtenida en **9.a**.
- VIP: dirección IP virtual a agregar.
  - Si agrega varias direcciones IP virtuales a la vez, sepárelas con las comas (,).
  - Si ya existe una dirección IP virtual y necesita agregar una nueva, el comando debe contener las direcciones IP virtuales nuevas y originales.

Comandos de ejemplo:

- Adición de una única dirección IP virtual: **nmcli connection modify "Wired connection 1" ipv4.addresses 172.16.0.125**
- Adición de múltiples direcciones IP virtuales: **nmcli connection modify "Wired connection 1" ipv4.addresses 172.16.0.125,172.16.0.126**

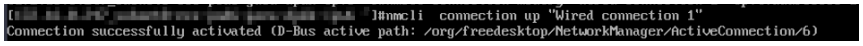
c. Ejecute el siguiente comando para hacer que la configuración entre en vigor:

nmcli connection up "*CONNECTION***"**

En este ejemplo, ejecute el siguiente comando:

nmcli connection up "Wired connection 1"

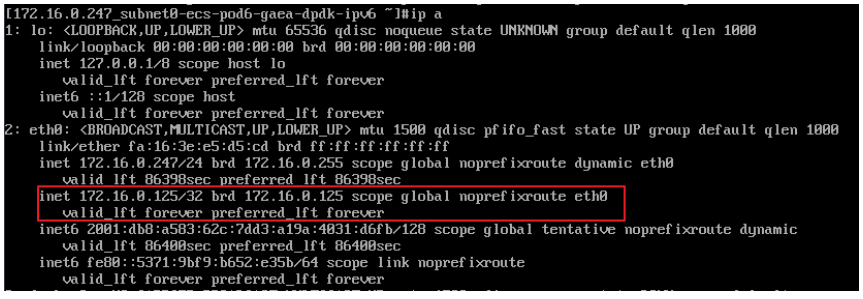
La información que aparecerá en pantalla será similar a la información siguiente:



d. Ejecute el siguiente comando para comprobar si la dirección IP virtual está enlazada:

ip a

Se muestra información similar a la siguiente. En la salida del comando, la dirección IP virtual 172.16.0.125 está vinculada a NIC eth0.



Windows OS (Windows Server se utiliza como ejemplo aquí.)

a. En **Control Panel**, haga clic en **Network and Sharing Center** y haga clic en la conexión local correspondiente.

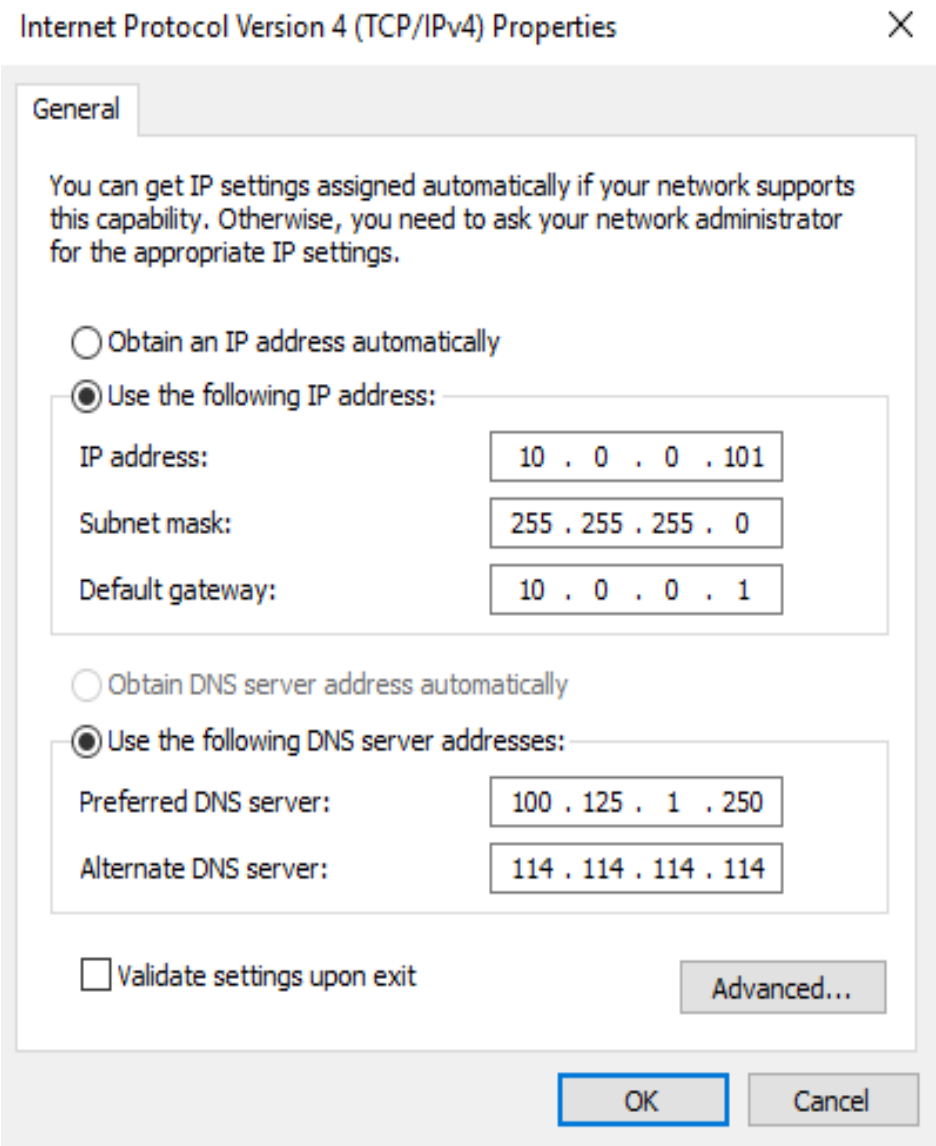
b. En la página mostrada, haga clic en **Properties**.

c. En la página **Network**, seleccione **Internet Protocol Version 4 (TCP/IPv4)**.

d. Haga clic en **Properties**.

e. Seleccione **Use the following IP address** y establecer **IP address** en la dirección IP privada del ECS, por ejemplo, 10.0.0.101.

Figura 9-3 Configuración de la dirección IP privada

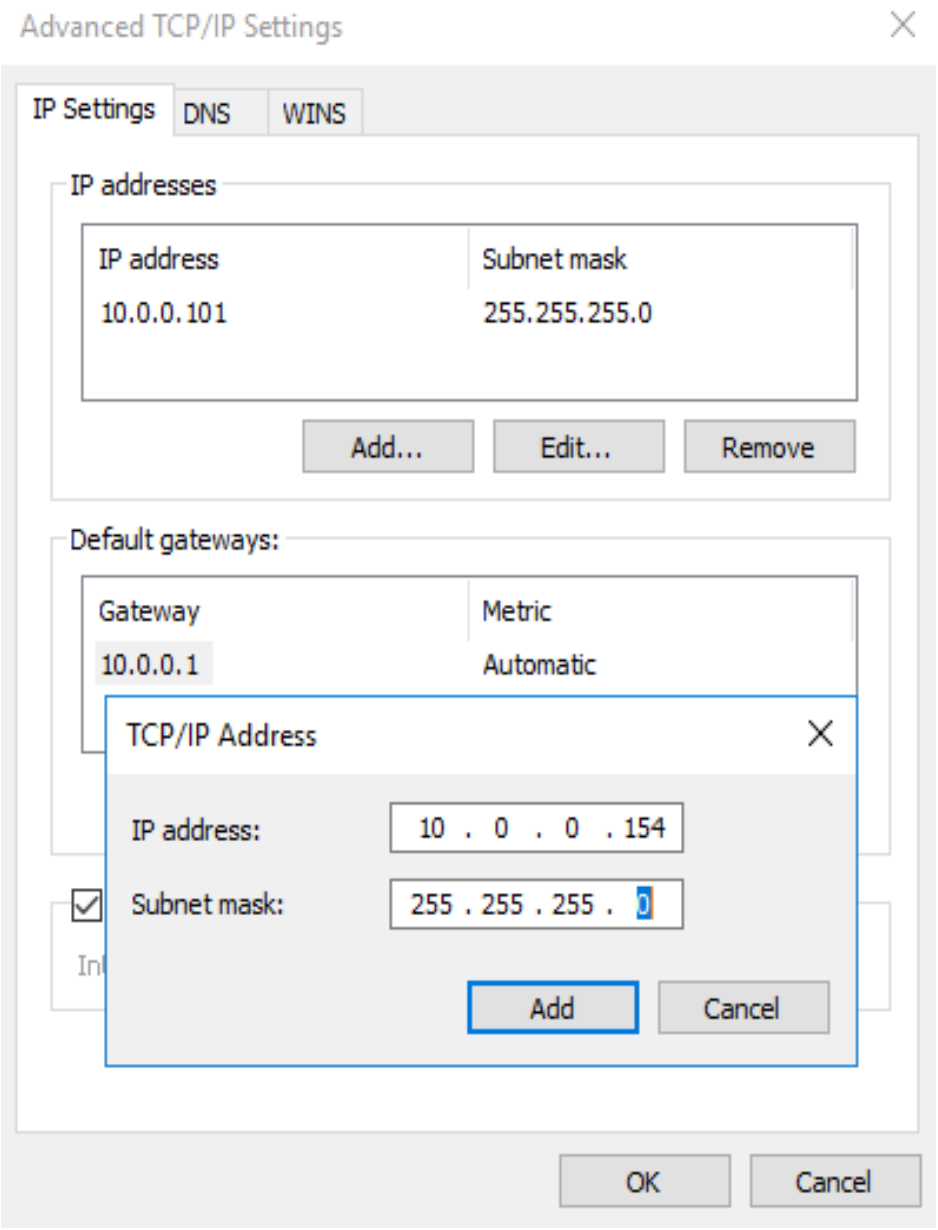


f. Haga clic en **Advanced**.

g. En la pestaña **IP Settings**, haga clic en **Add** en el área **IP addresses**.

Agrega la dirección IP virtual. Por ejemplo, 10.0.0.154.

Figura 9-4 Configuración de la dirección IP virtual



h. Haga clic en **OK**.

i. 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

En la salida del comando, **IPv4 Address** es la dirección IP virtual 10.0.0.154, que indica que la dirección IP virtual de la NIC de ECS se ha configurado correctamente.

9.4 Vinculación de una dirección IP virtual a una EIP

Escenarios

Esta sección describe cómo vincular una dirección IP virtual a una EIP.

Prerrequisitos

- Ha configurado la red ECS basada en **Redes** y asegúrese de que el ECS se ha enlazado con una dirección IP virtual.
- Ha asignado una EIP.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la página principal de la consola, en **Networking**, haga clic en **Elastic IP**.
4. Busque la fila que contiene el EIP que se va a enlazar a la dirección IP virtual y haga clic en **Bind** en la columna **Operation**.
5. En el cuadro de diálogo **Bind EIP**, establezca **Instance Type** en **Virtual IP address**.
6. En la lista de direcciones IP virtuales, seleccione la dirección IP virtual que desea vincular y haga clic en **OK**.

9.5 Uso de una VPN para acceder a una dirección IP virtual

Procedimiento

1. Configurar la red ECS basada en **Redes**.
2. Crear una VPN.

La VPN se puede utilizar para acceder a la dirección IP virtual del ECS.

9.6 Uso de una conexión de Direct Connect para acceder a la dirección IP virtual

Procedimiento

1. Configurar la red ECS basada en **Redes**.
2. Cree una conexión de Direct Connect.

La conexión de Direct Connect creada se puede utilizar para acceder a la dirección IP virtual del ECS.

9.7 Uso de una interconexión de VPC para acceder a la dirección IP virtual

Procedimiento

1. Configurar la red ECS basada en **Redes**.
2. Crear una interconexión de VPC.

Puede acceder a la dirección IP virtual del ECS a través de la interconexión de VPC.

9.8 Desactivación del reenvío de IP en el ECS en espera

Para un ECS de Linux:

1. Inicie sesión en ECS en standby y ejecute el siguiente comando para comprobar si el reenvío IP está habilitado:

   cat /proc/sys/net/ipv4/ip_forward

   En la salida del comando **1** indica que está habilitado y **0** indica que está deshabilitado. El valor predeterminado es **0**.

   – Si la salida del comando es **1**, realice **2** y **3** para deshabilitar el reenvío IP.

   – Si la salida del comando es **0**, no se requiere ninguna acción adicional.
2. Utilice el editor vi para abrir el archivo **/etc/sysctl.conf**, cambie el valor de **net.ipv4.ip_forward** a **0**, e introduzca **:wq** para guardar el cambio y salir. También puede utilizar el comando **sed** para modificar la configuración. Un ejemplo de comando es el siguiente:

   sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf
3. Ejecute el siguiente comando para hacer que el cambio surta efecto:

   sysctl -p /etc/sysctl.conf

Para un ECS de Windows:

1. Haga clic en **Start**, desplácese hacia abajo y expanda la carpeta **Windows System**, haga clic en **Command Prompt** y ejecute el siguiente comando:

   ipconfig /all

   En la salida del comando, si el valor de **IP Routing Enabled** es **No**, la función de reenvío IP está deshabilitada.
2. Presione las teclas **Windows** y **R** juntas para abrir el cuadro **Run** e introduzca **regedit** para abrir el **Registry Editor**.
3. Establezca el valor de **IPEnableRouter** en **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** en **0**.

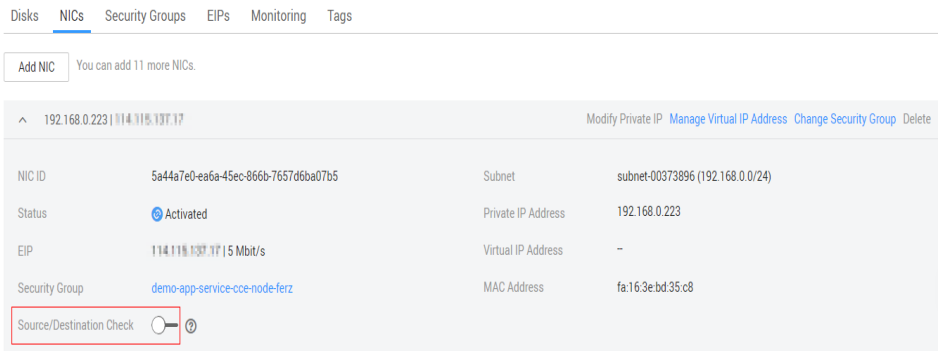
   – Si el valor se establece en **0**, se deshabilitará el reenvío de IP.

   – Si el valor se establece en **1**, se habilitará el reenvío IP.

9.9 Desactivación de la comprobación de origen y destino (escenario de clúster de equilibrio de carga HA)

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En **Compute**, haga clic en **Elastic Cloud Server**.
4. En la lista de ECS, haga clic en el nombre de ECS.
5. En la página de detalles de ECS que se muestra, haga clic en la ficha **NICs**.
6. Compruebe que **Source/Destination Check** esté deshabilitada.

Figura 9-5 Deshabilitar la comprobación de origen/destino



9.10 Lanzamiento de una dirección IP virtual

Scenarios

If you no longer need a virtual IP address or a reserved virtual IP address, you can release it to avoid wasting resources.

Prerequisites

Before deleting a virtual IP address, ensure that the virtual IP address has been unbound from the following resources:

- ECS
- EIP

Procedure

1. Log in to the management console.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. On the console homepage, under **Networking**, click **Virtual Private Cloud**.

4. In the navigation pane on the left, click **Subnets**.
5. In the subnet list, click the name of the subnet that the virtual IP address belongs to.
6. Click the **IP Addresses** tab, locate the row that contains the virtual IP address to be released, click **More** in the **Operation** column, and select **Release**.

Figura 9-6 Releasing a virtual IP address

7. Click **Yes** in the displayed dialog box.

10 Interconexión con CTS

10.1 Operaciones de VPC compatibles

Con CTS, puede registrar las operaciones realizadas en el servicio de VPC para fines de consulta, auditoría y seguimiento posterior.

Tabla 10-1 enumera las operaciones de VPC que pueden ser registradas por CTS.

Tabla 10-1 Operaciones de VPC que pueden ser grabadas por CTS

Operación	Tipo de recurso	Trazado
Modificación de un ancho de banda	Ancho de banda	modifyBandwidth
Asignación de una EIP	EIP	createEip
Lanzamiento de una EIP	EIP	deleteEip
Vinculación de una EIP	EIP	bindEip
Desvinculación de una EIP	EIP	unbindEip
Asignación de una dirección IP privada	Dirección IP privada	createPrivateIp
Eliminación de una dirección IP privada	Dirección IP privada	deletePrivateIp
Creación de un grupo de seguridad	security_groups	createSecurity-group
Actualización de un grupo de seguridad	security_groups	updateSecurity-group
Eliminación de un grupo de seguridad	security_groups	deleteSecurity-group
Creación de una regla de grupo de seguridad	security-group-rules	createSecurity-group-rule

Operación	Tipo de recurso	Trazado
Actualización de una regla de grupo de seguridad	security-group-rules	updateSecurity-group-rule
Eliminación de una regla de grupo de seguridad	security-group-rules	deleteSecurity-group-rule
Creación de una subred	Subnet	createSubnet
Supresión de una subred	Subnet	deleteSubnet
Modificación de una subred	Subnet	modifySubnet
Creación de una VPC.	VPC	createVpc
Eliminación de una VPC	VPC	deleteVpc
Modificación de una VPC	VPC	modifyVpc
Creación de una VPN	VPN	createVpn
Eliminación de una VPN	VPN	deleteVpn
Modificación de una VPN	VPN	modifyVpn
Creación de un router	routers	createRouter
Actualización de un router	routers	updateRouter
Adición de una interfaz a un router	routers	addRouterInterface
Eliminación de una interfaz de un router	routers	removeRouterInterface
Creación de un puerto	ports	createPort
Actualización de un puerto	ports	updatePort
Supresión de un puerto	ports	deletePort
Creación de una red	networks	createNetwork
Actualización de una red	networks	updateNetwork
Eliminación de una red	networks	deleteNetwork
Creación o eliminación de etiquetas de subred por lotes	tag	batchUpdateTags
Creación o eliminación de etiquetas de VPC por lotes	tag	batchUpdateVpcTags
Creación de una tabla de rutas	routetables	createRouteTable

Operación	Tipo de recurso	Trazado
Actualización de una tabla de rutas	routetables	updateRouteTable
Supresión de una tabla de ruta	routetables	deleteRouteTable
Creación de una interconexión de VPC	vpc-peerings	createVpcPeerings
Actualización de una interconexión de VPC	vpc-peerings	updateVpcPeerings
Eliminación de una interconexión de VPC	vpc-peerings	deleteVpcPeerings
Creación de un grupo de ACL de red	firewall-groups	createFirewallGroup
Actualización de un grupo de ACL de red	firewall-groups	updateFirewallGroup
Eliminación de un grupo de ACL de red	firewall-groups	deleteFirewallGroup
Creación de una política de ACL de red	firewall-policies	createFirewallPolicy
Actualización de una política de ACL de red	firewall-policies	updateFirewallPolicy
Eliminación de una política de ACL de red	firewall-policies	deleteFirewallPolicy
Inserción de una regla de ACL de red	firewall-policies	insertFirewallPolicyRule
Extracción de una regla de ACL de red	firewall-policies	removeFirewallPolicyRule
Creación de una regla de ACL de red	firewall-rules	createFirewallRule
Actualización de una regla de ACL de red	firewall-rules	updateFirewallRule
Eliminación de una regla de ACL de red	firewall-rules	deleteFirewallRule
Creación de un grupo de direcciones IP	address_group	createAddress_group
Actualización de un grupo de direcciones IP	address_group	updateAddress_group
Eliminación forzada de un grupo de direcciones IP	address_group	force_deleteAddress_group

Operación	Tipo de recurso	Trazado
Eliminación de un grupo de direcciones IP	address_group	deleteAddress_group
Creación de un log de flujo	flowlogs	createFlowLog
Actualización de un log de flujo	flowlogs	updateFlowLog
Eliminación de un log de flujo	flowlogs	deleteFlowLog

10.2 Consulta de trazas

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List**. En **Management & Governance**, haga clic en **Cloud Trace Service**.
4. En el panel de navegación de la izquierda, elija **Trace List**.
5. Especifique los filtros según sea necesario. Los siguientes filtros están disponibles:
   - **Trace Type**: Establezca en **Management** o **Data**.
   - **Trace Source**, **Resource Type**, y **Search By**

     Seleccione los filtros de la lista desplegable.

     Si selecciona **Trace name** para **Search By**, seleccione un nombre de seguimiento.

     If you select **Resource ID** for **Search By**, select or enter a resource ID.

     Si selecciona **Resource name** en **Search By**, seleccione o introduzca un nombre de recurso.
   - **Operator**: Seleccione un operador específico (un usuario que no sea una cuenta).
   - **Trace Status**: seleccione **All trace statuses**, **Normal**, **Warning**, o **Incident**.
   - Intervalo de tiempo de búsqueda: en la esquina superior derecha, elija **Last 1 hour**, **Last 1 day**, o **Last 1 week**, o especifique un intervalo de tiempo personalizado.
6. Haga clic en la flecha a la izquierda de la traza requerida para ampliar sus detalles.
7. Busque el seguimiento necesario y haga clic en **View Trace** en la columna **Operation**.

   Se muestra un cuadro de diálogo que muestra el contenido de seguimiento.

11 Monitoreo

11.1 Métricas admitidas

Descripción

Esta sección describe el espacio de nombres, la lista y las dimensiones de medición de las métricas de ancho de banda y EIP que puede comprobar en Cloud Eye. Puedes usar las API o la consola de Cloud Eye para consultar las métricas de las métricas monitorizadas y las alarmas generadas para EIP y anchos de banda.

Espacio de nombres

SYS.VPC

Métricas de monitoreo

Tabla 11-1 EIP y métricas de ancho de banda

ID	Nombre	Descripción	Rango de valores	Objeto monitoreado	Intervalo de supervisión (datos brutos)
upstream_bandwidth	Outbound Bandwidth	Velocidad de red del tráfico saliente (anteriormente llamado "Upstream Bandwidth") Unidad: bit/s	≥ 0 bit/s	Ancho de banda o EIP	1 minuto

ID	Nombre	Descripción	Rango de valores	Objeto monitoreado	Intervalo de supervisión (datos brutos)
downstream_bandwidth	Inbound Bandwidth	Velocidad de red del tráfico entrante (anteriormente llamado "Downstream Bandwidth") Unidad: bit/s	≥ 0 bit/s	Ancho de banda o EIP	1 minuto
upstream_bandwidth_usage	Outbound Bandwidth Usage	Uso del ancho de banda saliente en la unidad de porcentaje.	0% a 100%	Ancho de banda o EIP	1 minuto
up_stream	Outbound Traffic	Tráfico de red que sale de la plataforma en la nube (anteriormente llamado "Upstream Traffic") Unidad: byte	≥ 0 bytes	Ancho de banda o EIP	1 minuto
down_stream	Inbound Traffic	Tráfico de red que va a la plataforma en la nube (anteriormente llamado "Downstream Traffic") Unidad: byte	≥ 0 bytes	Ancho de banda o EIP	1 minuto

Dimensiones

Clave	Valor
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

Si un objeto supervisado tiene varias dimensiones, todas las dimensiones son obligatorias cuando usas API para consultar las métricas.

- Consultar una métrica de supervisión:

  dim.0=bandwidth_id,530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id,3773b058-5b4f-4366-9035-9bbd9964714a

- Consultar las métricas de supervisión por lotes:

  "dimensions": [

  {

  "name": "bandwidth_id",

  "value": "530cd6b0-86d7-4818-837f-935f6a27414d"

  }

  {

  "name": "publicip_id",

  "value": "3773b058-5b4f-4366-9035-9bbd9964714a"

  }

  ],

11.2 Consulta de métricas

Escenarios

Vea las métricas relacionadas para ver el ancho de banda y la información de uso de EIP.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Pase el ratón por la esquina superior izquierda para mostrar **Service List** y elija **Management & Deployment** > **Cloud Eye**.
4. Haga clic en **Cloud Service Monitoring** a la izquierda de la página y elija **Elastic IP and Bandwidth**.
5. Busque la fila que contiene el ancho de banda de destino o EIP y haga clic en **View Metric** en la columna **Operation** para comprobar la información de supervisión del ancho de banda o EIP.

11.3 Creación de una regla de alarma

Escenarios

Puede configurar reglas de alarma para personalizar los objetos supervisados y las políticas de notificación. Puede conocer los estados de sus recursos en cualquier momento.

Procedimiento

1. Inicie sesión en la consola de gestión.

2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Pase el ratón por la esquina superior izquierda para mostrar **Service List** y elija **Management & Deployment** > **Cloud Eye**.
4. En el panel de navegación izquierdo de la izquierda, elija **Alarm Management** > **Alarm Rules**.
5. En la página **Alarm Rules**, haga clic en **Create Alarm Rule** y establezca los parámetros necesarios o modifique una regla de alarma existente.
6. Después de establecer los parámetros, haga clic en **Create**.

   Una vez creada la regla de alarma, el sistema le notifica automáticamente si se activa una alarma para el servicio de VPC.

12 Gestión de permisos

12.1 Creación de un usuario y concesión de permisos de VPC

Esta sección describe cómo usar IAM para implementar un control de permisos detallado para los recursos de VPC. Con IAM, usted puede:

- Crear usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tendrá sus propias credenciales de seguridad para acceder a los recursos de VPC.
- Conceder sólo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confíe en una cuenta de Huawei Cloud o un servicio en la nube para realizar O&M eficientes en sus recursos de VPC.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM, omita esta sección.

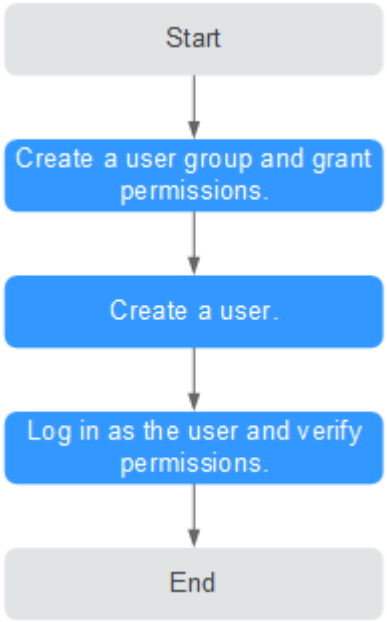
En esta sección se describe el procedimiento para conceder permisos (consulte **Figura 12-1**).

Prerrequisitos

Más información sobre los permisos compatible con VPC y elija políticas o roles de acuerdo con sus requisitos. Para obtener los permisos de otros servicios.

Flujo del proceso

Figura 12-1 Proceso para conceder permisos de VPC



1. **Crear un grupo de usuarios y concederle los permisos.**

   Cree un grupo de usuarios en la consola de IAM y asigne la política **VPC ReadOnlyAccess** al grupo.
2. **Crear un usuario de IAM.**

   Cree un usuario en la consola de IAM y agregue el usuario al grupo creado en **1**.
3. **Iniciar sesión** y verificar los permisos.

   Inicie sesión en la consola de VPC mediante el usuario creado en 2, y compruebe que el usuario solo tiene permisos de lectura para VPC.
   - Elija **Service List** > **Virtual Private Cloud**. A continuación, haga clic en **Create VPC** en la consola de VPC. Si aparece un mensaje que indica que no tiene permisos suficientes para realizar la operación, la política **VPC ReadOnlyAccess** ya tiene efecto.
   - Elija cualquier otro servicio en el **Service List**. Si aparece un mensaje que indica que no tiene permisos suficientes para acceder al servicio, la política **VPC ReadOnlyAccess** ya ha entrado en vigor.

12.2 Políticas personalizadas de VPC

Se pueden crear las políticas personalizadas para complementar las políticas definidas por el sistema de VPC. Para ver las acciones admitidas para las políticas personalizadas.

Puede crear las políticas personalizadas de cualquiera de las siguientes maneras:

- Visual editor: Seleccione servicios en la nube, acciones, recursos y condiciones de solicitud. Esto no requiere conocimiento de la sintaxis de políticas.
- JSON: Edite las políticas JSON desde cero o basándose en una política existente.

Para obtener detalles sobre la operación La siguiente sección contiene los ejemplos de las políticas personalizadas comunes de VPC.

Ejemplo de las políticas personalizadas

- Ejemplo 1: Permitir a los usuarios crear y consultar las VPC

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                     vpc:vpcs:create
                     vpc:svpcs:list
                 "
            ]
        }
    ]
}
```

- Ejemplo 2: Denegación de la eliminación de VPC

  Una política de denegación debe usarse junto con otras políticas para que surtan efecto. Si los permisos asignados a un usuario contienen acciones Allow y Deny, las acciones Deny tienen prioridad sobre las acciones Allow.

  El siguiente método se puede utilizar si necesita asignar permisos de la política **VPC FullAccess** a un usuario, pero también prohibir que el usuario elimine VPC. Cree una política personalizada para denegar la eliminación de VPC y asigne ambas políticas al grupo al que pertenece el usuario. A continuación, el usuario puede realizar todas las operaciones en la VPC, excepto eliminar las VPC. El seguiente se muestra un ejemplo de política de denegación:

```
{
      "Version": "1.1",
      "Statement": [
            {
          "Effect": "Deny",
                  "Action": [
                        "vpc:vpcs:delete"
                  ]
            }
      ]
}
```

- Ejemplo 3: Definición de permisos para varios servicios en una política

  Una política personalizada puede contener las acciones de varios servicios que son de tipo global o de nivel de proyecto. A continuación se muestra una política de ejemplo que contiene acciones de varios servicios:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "vpc:vpcs:create",
                "vpc:vpcs:update"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ecs:servers:delete"
            ],
            "Effect": "Allow"
        }
```



```
    ]
}
```

