

# Virtual Private Network

## Guía de usuario

Edición 01  
Fecha 2023-01-11



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

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

## **Marcas y permisos**



HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.

Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

## **Aviso**

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

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

# Índice

<b>1 Guía de usuario.....</b>	<b>1</b>
1.1 Gestión de puerta de enlace de VPN.....	1
1.1.1 Ver una puerta de enlace VPN.....	1
1.1.2 Modificación de un gateway de VPN.....	1
1.1.3 Vinculación de un EIP a una puerta de enlace de VPN.....	2
1.1.4 Desvincular un EIP de una puerta de enlace de VPN.....	2
1.1.5 Cancelación de la suscripción de una puerta de enlace VPN anual/mensual.....	3
1.1.6 Eliminación de una puerta de enlace de VPN de pago por uso.....	4
1.2 Gestión de la puerta de enlace del cliente.....	4
1.2.1 Consulta de una puerta de enlace de cliente.....	4
1.2.2 Modificación de una puerta de enlace de cliente.....	5
1.2.3 Eliminación de una puerta de enlace de cliente.....	5
1.3 Gestión de conexiones VPN.....	6
1.3.1 Visualización de una conexión de VPN.....	6
1.3.2 Modificación de una conexión de VPN.....	6
1.3.3 Eliminación de una conexión de VPN.....	8
1.4 Gestión de la puerta de enlace de Classic VPN 1.1.....	8
1.4.1 Ver una puerta de enlace VPN.....	9
1.4.2 Modificación de un gateway de VPN.....	9
1.4.3 Cancelación de la suscripción de una puerta de enlace VPN anual/mensual.....	10
1.4.4 Eliminación de una puerta de enlace de VPN de pago por uso.....	10
1.5 Classic VPN 1.1 Gestión de conexiones.....	11
1.5.1 Visualización de una conexión de VPN.....	11
1.5.2 Modificación de una conexión de VPN.....	11
1.5.3 Eliminación de una conexión de VPN.....	12
1.6 Gestión de Classic VPN 1.0.....	12
1.6.1 Consulta de VPNs clásicas compradas.....	12
1.6.2 Modificación de una VPN clásica comprada.....	13
1.6.3 Eliminación de un Classic VPN.....	14
1.7 Monitoreo.....	14
1.7.1 Monitoreo de VPN.....	14
1.7.2 Métricas.....	14
1.7.3 Visualización de las métricas.....	17

---

1.7.4 Creación de reglas de alarma.....	19
1.8 Operaciones clave registradas por CTS.....	20
1.8.1 Operaciones de VPN que pueden ser registradas por CTS.....	20
1.8.2 Consulta de rastros de CTS.....	21
1.9 Gestión de permisos.....	22
1.9.1 Creación de un usuario y concesión de permisos VPN.....	22
1.9.2 Políticas personalizadas de VPN.....	23
1.10 Cuotas.....	25

# 1 Guía de usuario


## 1.1 Gestión de puerta de enlace de VPN

### 1.1.1 Ver una puerta de enlace VPN


#### Escenarios

Después de crear una puerta de enlace VPN, puede ver sus detalles.

#### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. En la página **VPN Gateways**, vea la lista de puerta de enlace VPN.
6. Haga clic en el nombre de una puerta de enlace VPN para ver su información básica y direcciones IP públicas.



En la lista de puerta de enlace VPN, puede localizar la conexión VPN de destino y hacer clic en  para ver el ancho de banda y el tráfico de la puerta de enlace VPN.

### 1.1.2 Modificación de un gateway de VPN

#### Escenarios



- Puede modificar la información básica sobre una puerta de enlace VPN, incluidos el nombre y las subredes locales.

## Modificación de información básica

### Escenario

Puede modificar el nombre y la subred local de una puerta de enlace VPN.

### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino y haga clic en **Modify Basic Information** en la columna **Operation**.  
Para modificar solo el nombre de una puerta de enlace VPN, también puede hacer clic en  junto al nombre de la puerta de enlace VPN.
6. Modifique el nombre y la subred local de la puerta de enlace VPN según se le solicite.
7. Haga clic en **OK**.

## 1.1.3 Vinculación de un EIP a una puerta de enlace de VPN

### Escenarios

Puede vincular un EIP a una puerta de enlace VPN que se haya creado.

### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino y haga clic en **Bind EIP** en la columna **Operation**.  
Una puerta de enlace de VPN puede tener un EIP activo y un EIP en espera unidos.
6. Seleccione el EIP deseado y haga clic en **OK**.

## 1.1.4 Desvincular un EIP de una puerta de enlace de VPN

### Escenarios

Después de crear una puerta de enlace de VPN, puede desvincular un EIP de ella.

## 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino y haga clic en **Unbind EIP** en la columna **Operation**.

Puede desvincular el EIP activo o en espera, o ambos, desde la puerta de enlace VPN.

6. En el cuadro de diálogo que se muestra, haga clic en **Yes**.



- Un EIP que está en uso por una conexión VPN no se puede separar de una puerta de enlace VPN.
- Un EIP continuará siendo facturado después de estar desvinculado de una puerta de enlace de VPN. Si ya no necesita una EIP, se le aconseja que la libere.

## 1.1.5 Cancelación de la suscripción de una puerta de enlace VPN anual/mensual


### Escenarios

Si ya no se requiere una puerta de enlace VPN anual/mensual, puede cancelar su suscripción.



- No tiene que crear una conexión VPN junto con una puerta de enlace VPN anual/mensual.
- Darse de baja de una puerta de enlace anual/mensual también eliminará las conexiones VPN creadas para la puerta de enlace. Por lo tanto, realice esta operación con precaución.

## 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 el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
4. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino y elija **More > Unsubscribe** en la columna **Operation**.
5. Cancelar la suscripción de la puerta de enlace VPN como se le solicite.

## 1.1.6 Eliminación de una puerta de enlace de VPN de pago por uso


### Escenarios

Puede eliminar una puerta de enlace VPN de pago por uso que ya no sea necesaria.

### Restricciones y limitaciones

- Una puerta de enlace VPN solo se puede eliminar cuando está en estado normal o anormal.
- Si una puerta de enlace VPN tiene conexiones VPN configuradas, debe eliminar todas las conexiones VPN antes de eliminar la puerta de enlace VPN.  
Para obtener más información sobre cómo eliminar una conexión VPN, consulte [Eliminación de una conexión de VPN](#).
- Si una puerta de enlace de VPN está vinculada a un EIP facturado en modo anual/mensual, debe desvincular el EIP antes de eliminar la puerta de enlace de VPN.  
Para obtener más información sobre cómo desvincular un EIP, consulte [Desvincular un EIP de una puerta de enlace de VPN](#).
- Si una puerta de enlace de VPN está vinculada a un EIP facturado en modo de pago por uso, la eliminación de la puerta de enlace de VPN también eliminará el EIP.  
Para conservar tal EIP de pago por uso, desvíelo antes de eliminar la puerta de enlace VPN. Para obtener más información sobre cómo desvincular un EIP, consulte [Desvincular un EIP de una puerta de enlace de VPN](#).

### 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 el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
4. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino y elija **More > Delete** en la columna **Operation**.
5. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

## 1.2 Gestión de la puerta de enlace del cliente


### 1.2.1 Consulta de una puerta de enlace de cliente

#### Escenarios

Después de crear una puerta de enlace de cliente, puede ver sus detalles.



## 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > Customer Gateways**.
5. En la página **Customer Gateway**, vea la lista de puerta de enlace del cliente.

## 1.2.2 Modificación de una puerta de enlace de cliente

### Escenarios

Después de crear una puerta de enlace de cliente, puede cambiar su nombre.

### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > Customer Gateways**.
5. En la página **Customer Gateway**, haga clic en  junto al nombre de una puerta de enlace de cliente.
6. Introduzca un nuevo nombre para la puerta de enlace del cliente y haga clic en **OK**.

## 1.2.3 Eliminación de una puerta de enlace de cliente

### Escenarios

Puede eliminar una puerta de enlace de cliente que haya creado.

### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > Customer Gateways**.
5. En la página **Customer Gateway**, busque la puerta de enlace del cliente que desea eliminar y haga clic en **Delete** en la columna **Operation**.  
Antes de eliminar una puerta de enlace de cliente asociada a una conexión VPN, elimine la puerta de enlace de cliente de la conexión VPN.

6. Haga clic en **Yes**.


## 1.3 Gestión de conexiones VPN

### 1.3.1 Visualización de una conexión de VPN

#### Escenarios

Después de crear una conexión VPN, puede ver sus detalles.

#### Procedimiento

1. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
2. Haga clic en **Service List** y elija **Networking > Virtual Private Network**.
3. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Connections**.
4. En la página **VPN Connections**, vea la lista de conexiones VPN.
5. Haga clic en el nombre de una conexión VPN para ver su información básica.




- En la página Detalles de la conexión VPN, puede hacer clic en **Modify Policy Settings** para ver detalles sobre las directivas IKE e IPsec de la conexión VPN.
- En la lista de conexiones VPN, puede localizar la conexión VPN de destino y hacer clic en **View Metric** para ver la información de supervisión sobre la conexión VPN.

### 1.3.2 Modificación de una conexión de VPN

#### Escenarios

Una conexión VPN es un canal de comunicaciones cifrado establecido entre una puerta de enlace VPN en una VPC y una puerta de enlace de cliente en su centro de datos local. Puede modificar una conexión VPN cuando sea necesario.

#### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Connections**.
5. En la página **VPN Connections**, busque la conexión VPN que desea modificar y haga clic en **Modify VPN Connection**.
6. Modifique los parámetros de conexión VPN según se le solicite.

7. Haga clic en **OK**.



Si cambia la PSK o modifica la política IKE o IPsec de una conexión VPN, asegúrese de que las nuevas configuraciones sean consistentes con las de la puerta de enlace del cliente. De lo contrario, se interrumpirá la conexión VPN.

- **Cambio del PSK**  
 Localice la conexión VPN que desea modificar, elija **More > Reset PSK** a la derecha y cambie el PSK según se le solicite. El nuevo PSK entra en vigor inmediatamente después de ser configurado.
- **Modificación de la política de IKE**  
 Busque la conexión VPN que desea modificar, elija **More > Modify Policy Settings** a la derecha y modifique las directivas IKE e IPsec según se le solicite.  
 Solo algunos de los parámetros tienen efecto inmediatamente después de ser modificados, como se describe en [Tabla 1-1](#).

**Tabla 1-1** Hora en que entran en vigor los nuevos ajustes de parámetros

¿Hacer efecto inmediata mente?	Parámetro de política de IKE	Parámetro de política de IPsec	Descripción
Sí	<ul style="list-style-type: none"> <li>● Version</li> <li>● Negotiation Mode This parameter is available only when <b>Version</b> is v1.</li> <li>● Lifetime (s)</li> <li>● Local ID</li> <li>● Customer ID</li> </ul>	<ul style="list-style-type: none"> <li>● Transfer Protocol</li> <li>● Lifetime (s)</li> </ul>	-


¿Hacer efecto inmediatamente?	Parámetro de política de IKE	Parámetro de política de IPsec	Descripción
No	<ul style="list-style-type: none"> <li>● Authentication Algorithm</li> <li>● Encryption Algorithm</li> <li>● DH Algorithm</li> </ul>	<ul style="list-style-type: none"> <li>● Authentication Algorithm</li> <li>● Encryption Algorithm</li> <li>● PFS</li> </ul>	<ul style="list-style-type: none"> <li>● Cuando la conexión VPN está en estado <b>Connected</b>: La nueva configuración del algoritmo entrará en vigor en el siguiente ciclo de vida de la política correspondiente.</li> <li>● Cuando la conexión VPN está en estado <b>Not connected</b>: La renegociación IPsec se realiza repetidamente, por lo que la configuración de los parámetros tiene efecto inmediatamente.</li> </ul>

### 1.3.3 Eliminación de una conexión de VPN

#### Escenarios

Si ya no se necesita una conexión VPN, puede eliminarla para liberar recursos 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. Haga clic en **Service List** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Connections**.
5. En la página **VPN Connections**, elija **More > Delete** en la columna **Operation** de una conexión VPN.
6. En el cuadro de diálogo que se muestra, haga clic en **Yes**.


## 1.4 Gestión de la puerta de enlace de Classic VPN 1.1

## 1.4.1 Ver una puerta de enlace VPN

### Escenarios

Después de crear una puerta de enlace VPN, puede ver sus detalles.

### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. Vea información sobre su puerta de enlace VPN.


## 1.4.2 Modificación de un gateway de VPN

### Modificación de información básica sobre una puerta de enlace VPN

#### Escenario

Puede modificar el nombre y la descripción de una puerta de enlace VPN.

#### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN que desea modificar y elija **More > Modify Basic Information** en la columna **Operation**.
6. Modifique el nombre o la descripción de la puerta de enlace VPN según sea necesario.
7. Haga clic en **OK**.

### Modificación del ancho de banda de la puerta de enlace VPN

#### Escenario

Cuando el ancho de banda de una puerta de enlace VPN no puede cumplir con sus requisitos de servicio, puede modificar el ancho de banda de la puerta de enlace VPN.

#### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino y elija **More > Modify Bandwidth** en la columna **Operation**.
6. Modifique el ancho de banda según sea necesario.
7. Haga clic en **Submit**.

### 1.4.3 Cancelación de la suscripción de una puerta de enlace VPN anual/mensual


#### Escenarios

Si ya no se requiere una puerta de enlace VPN anual/mensual, puede cancelar su suscripción.



- No tiene que crear una conexión VPN junto con una puerta de enlace VPN anual/mensual.
- Darse de baja de una puerta de enlace anual/mensual también eliminará las conexiones VPN creadas para la puerta de enlace. Por lo tanto, realice esta operación con precaución.

#### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino y elija **More > Unsubscribe** en la columna **Operation**.
6. Cancelar la suscripción de la puerta de enlace VPN como se le solicite.

### 1.4.4 Eliminación de una puerta de enlace de VPN de pago por uso

#### Escenarios


Si ya no se necesita una puerta de enlace VPN, puede eliminarla para liberar recursos de red siempre que no tenga conexiones VPN configuradas.

Si tiene alguna conexión configurada, elimine primero las conexiones.



Si crea una puerta de enlace de VPN de pago por uso, se creará una conexión VPN junto con la puerta de enlace. Si elimina todas las conexiones VPN creadas para una puerta de enlace de VPN de pago por uso, la puerta de enlace de VPN se eliminará automáticamente. Para más detalles, consulte [Eliminación de una conexión de VPN](#).

## 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 el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Gateways**.
4. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN de destino. En la columna **Operation**, elija **More > Delete**.
5. En el cuadro de diálogo que se muestra, haga clic en **Yes**.


## 1.5 Classic VPN 1.1 Gestión de conexiones

### 1.5.1 Visualización de una conexión de VPN

#### Escenarios

Después de crear una conexión VPN, puede ver sus detalles.

#### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Connections**.
5. En la página **VPN Connections**, vea la información de conexión VPN. También puede buscar la fila que contiene la conexión VPN de destino y, en la columna **Operation**, haga clic en **View Policy** para ver los detalles de la política IKE e IPsec sobre la conexión VPN.

### 1.5.2 Modificación de una conexión de VPN

#### Escenarios

Una conexión VPN es un canal de comunicaciones encriptado establecido entre la puerta de enlace VPN de su VPC y la de un centro de datos local. La conexión VPN se puede modificar después de la creación.




Si modifica la configuración avanzada, es posible que se interrumpan las comunicaciones de red. Tenga cuidado al realizar esta operación.

La modificación de la PSK solamente no eliminará la conexión VPN actual. La nueva PSK entra en vigor durante la renegociación de IKE después de que expire el ciclo de vida de IKE.

---

## 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Connections**.
5. En la página **VPN Connections**, busque la fila que contiene la conexión VPN de destino y haga clic en **Modify** en la columna **Operation**.
6. En el cuadro de diálogo **Modify VPN Connection** que se muestra, modifique los parámetros según sea necesario.
7. Haga clic en **OK**.


### 1.5.3 Eliminación de una conexión de VPN

#### Escenarios

Si ya no se necesita una conexión VPN, puede eliminarla para liberar recursos de red.

Cuando elimina la última conexión VPN de una puerta de enlace VPN de pago por uso, también se eliminará la puerta de enlace VPN asociada.

#### 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** y elija **Networking > Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network > VPN Connections**.
5. En la página **VPN Connections**, busque la fila que contiene la conexión VPN. En la columna **Operation**, elija **More > Delete**.
6. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

## 1.6 Gestión de Classic VPN 1.0

### 1.6.1 Consulta de VPNs clásicas compradas


#### Escenarios

Esta sección se aplica a las regiones donde se utiliza Classic VPN 1.0.

Puede ver detalles sobre una VPN existente.



## 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** y elija **Networking > Virtual Private Network**.
4. En la página **Virtual Private Network** mostrada, vea la VPN de destino. [Tabla 1-2](#) describe el estado de la VPN.

**Tabla 1-2** Estado de VPN

Estado	Descripción
Normal	La VPN se crea con éxito y las comunicaciones entre la VPC y el centro de datos local son normales.
Not connected	La VPN se ha creado correctamente, pero no se ha utilizado para las comunicaciones con el centro de datos local.
Creating	Se está creando la VPN.
Updating	La información de VPN se está actualizando.
Deleting	La VPN se está eliminando.
Abnormal	La VPN es anormal.
Frozen	La VPN está congelada.


## 1.6.2 Modificación de una VPN clásica comprada

### Escenarios

Esta sección se aplica a las regiones donde se utiliza Classic VPN 1.0.

Si la información de la red VPN entra en conflicto con la información de la red VPC o necesita ajustarse en función del entorno de red más reciente, puede modificar la VPN.

### 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** y elija **Networking > Virtual Private Network**.
4. En la página **Virtual Private Network**, localice la VPN de destino y haga clic en **Modify**.
5. En el cuadro de diálogo mostrado, modifique los parámetros según sea necesario.
6. Haga clic en **OK**.


## 1.6.3 Eliminación de un Classic VPN

### Escenarios

Esta sección se aplica a las regiones donde se utiliza Classic VPN 1.0.

Puede eliminar una VPN si ya no es 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. Haga clic en **Service List** y elija **Networking > Virtual Private Network**.
4. En la página **Virtual Private Network**, localice la VPN de destino y haga clic en **Delete**.
5. En el cuadro de diálogo que se muestra, haga clic en **Yes**.

## 1.7 Monitoreo

### 1.7.1 Monitoreo de VPN

Cloud Eye le permite vigilar de cerca el rendimiento y la utilización de recursos de las VPN, lo que garantiza la confiabilidad y disponibilidad de las VPN. Puede usar Cloud Eye para monitorear automáticamente las VPN en tiempo real y gestionar alarmas y notificaciones, para que pueda realizar un seguimiento de las métricas de rendimiento de la VPN.



Esta función solo es compatible con VPN y Classic VPN 1.1, pero no con Classic VPN 1.0.

### 1.7.2 Métricas

#### Descripción

En esta sección se describen las métricas monitoreadas notificadas por VPN a Cloud Eye, así como sus espacios de nombres y dimensiones. Puede utilizar la consola de gestión de Cloud Eye para consultar las métricas de los objetos supervisados y las alarmas generadas para VPN.

#### Espacio de nombres

SYS.VPN

## Métricas

**Tabla 1-3** Métricas de conexión VPN

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
private_average_latency	private network average Round-Trip Time	Average round-trip time (RTT) entre la dirección de interfaz de túnel de la puerta de enlace de VPN y la de la puerta de enlace del cliente	0 - 5000 ms	Conexión de VPN	1 minuto
private_max_latency	private network maximum Round-Trip Time	RTT máximo entre la dirección de interfaz de túnel de la puerta de enlace de VPN y la de la puerta de enlace del cliente	0 - 5000 ms	Conexión de VPN	1 minuto
private_packet_loss_rate	private network packet loss rate	Tasa de pérdida de paquetes entre la dirección de interfaz de túnel de la puerta de enlace VPN y la de la puerta de enlace del cliente	0 - 100 %	Conexión de VPN	1 minuto
public_average_latency	public network average Round-Trip Time	RTT promedio entre la dirección IP pública de la pasarela VPN y la de la pasarela del cliente	0 - 5000 ms	Conexión de VPN	1 minuto
public_max_latency	public network maximum Round-Trip Time	RTT máximo entre la dirección IP pública de la pasarela VPN y la de la pasarela del cliente	0 - 5000 ms	Conexión de VPN	1 minuto
public_packet_loss_rate	public network packet loss rate	Tasa de pérdida de paquetes entre la dirección IP pública de la pasarela VPN y la de la pasarela del cliente	0 - 100 %	Conexión de VPN	1 minuto

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
connection_status	VPN Connection Status	Estado de conexión VPN: <b>0</b> : Una conexión VPN está en estado <b>Not connected</b> . <b>1</b> : Una conexión VPN está en estado <b>Connected</b> .	0 o 1	Conexión de VPN	1 minuto

**Tabla 1-4** Métricas de conexión de Classic VPN

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
connection_status	VPN Connection Status	Estado de conexión VPN: <b>0</b> : Una conexión VPN está en estado <b>Not connected</b> . <b>1</b> : Una conexión VPN está en estado <b>Connected</b> .	0 o 1	Conexión de VPN	5 minutos

**Tabla 1-5** Métricas de pasarela VPN

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
upstream_bandwidth	Outbound Bandwidth	Velocidad de red del tráfico saliente (anteriormente llamado "ancho de banda ascendente") Unidad: bit/s	$\geq 0$ bit/s	Ancho de banda o EIP	1 minuto
downstream_bandwidth	Inbound Bandwidth	Velocidad de red del tráfico entrante (anteriormente llamado "ancho de banda descendente") Unidad: bit/s	$\geq 0$ bit/s	Ancho de banda o EIP	1 minuto

ID de métrica	Nombre de la métrica	Descripción	Rango de valores	Objeto monitoreado	Intervalo de monitoreo (datos brutos)
upstream_bandwidth_usage	Outbound Bandwidth Usage	Uso del ancho de banda saliente, en porcentaje.	0-100%	Ancho de banda o EIP	1 minuto
downstream_bandwidth_usage	Inbound Bandwidth Usage	Uso del ancho de banda entrante, en porcentaje.	0-100%	Ancho de banda o EIP	1 minuto
upstream	Outbound Traffic	Tráfico de red saliente (anteriormente denominado "Tráfico ascendente") Unidad: byte	$\geq 0$ bytes	Ancho de banda o EIP	1 minuto
downstream	Inbound Traffic	Tráfico de red entrante (anteriormente denominado "Tráfico descendente") Unidad: byte	$\geq 0$ bytes	Ancho de banda o EIP	1 minuto

## Dimensiones

Clave	Valor
connection_id	VPN Connections
vpn_connection_id	Dedicated Connections
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

### 1.7.3 Visualización de las métricas

#### Escenarios



Vea el estado de la conexión VPN y los usos del ancho de banda y EIP.


## Contexto

**Tabla 1-6** Soporte para métricas

Nombre de la métrica	Soporte	¿Habilitado por defecto?	Restricción
VPN Connection Status	Soportado tanto por VPN como por Classic VPN	Sí	Ninguno
<ul style="list-style-type: none"> <li>● public network average Round-Trip Time</li> <li>● public network maximum Round-Trip Time</li> <li>● public network packet loss rate</li> </ul>	Soportado solo por VPN	No Puede hacer clic en el nombre de una conexión VPN y agregar un elemento de comprobación de estado en la página de pestaña <b>Summary</b> .	Ninguno
<ul style="list-style-type: none"> <li>● private network average Round-Trip Time</li> <li>● private network maximum Round-Trip Time</li> <li>● private network packet loss rate</li> </ul>	Soportado solo por VPN	No Puede hacer clic en el nombre de una conexión VPN y agregar un elemento de comprobación de estado en la página de pestaña <b>Summary</b> .	Las métricas solo se pueden configurar cuando una conexión VPN utiliza el modo de enrutamiento estático y tiene NQA habilitado.

## Consulta de Métricas de Conexión de VPN


- Consulta de métricas en la consola VPN
  - a. Inicie sesión en la consola de gestión.
  - b. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
  - c. Haga clic en **Service List** y elija **Networking > Virtual Private Network**.
  - d. Elija **Virtual Private Network > VPN Connections**.  
Para VPN clásica, elija **Virtual Private Network > Classic VPNs**, y haga clic en la pestaña **VPN Connections**.
  - e. Busque la conexión VPN de destino y haga clic en el icono **View Metric** .  
Para VPN clásica, localice la conexión VPN de destino y haga clic en **View Metric** en la columna **Operation**.  
Puede ver los datos de las últimas 1, 3, 12 o 24 horas, o los últimos 7 días.
- Consulta de métricas en la consola de Cloud Eye
  - a. Inicie sesión en la consola de gestión.


- b. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
- c. Haga clic en **Service List** y elija **Management & Governance > Cloud Eye**.
- d. Elija **Cloud Service Monitoring > Virtual Private Network**.
- e. Haga clic en la pestaña **Dedicated Connections**, busque la conexión VPN de destino y haga clic en **View Metric** en la columna **Operation**.

Para VPN clásica, haga clic en la pestaña **VPN Connections**, busque la conexión VPN de destino y haga clic en **View Metric** en la columna **Operation**.


Puede ver los datos de las últimas 1, 3, 12 o 24 horas, o los últimos 7 días.

## Consulta de Métricas de puerta de enlace de VPN

- Consulta de métricas en la consola VPN (recomendado)
  - a. Inicie sesión en la consola de gestión.
  - b. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
  - c. Haga clic en **Service List** y elija **Networking > Virtual Private Network**.
  - d. Elija **Virtual Private Network > VPN Gateways**.

Para Classic VPN, elija **Virtual Private Network > Classic VPNs**, y haga clic en la pestaña **VPN Gateways**.
  - e. Localice la puerta de enlace VPN de destino y haga clic en  en la columna **Public IP Address** para ver los datos de supervisión de EIP de la puerta de enlace VPN.

Para VPN clásica, localice la puerta de enlace VPN de destino y haga clic en **View Metric** en la columna **Operation** para ver los datos de supervisión de EIP de la puerta de enlace VPN.

Puede ver los datos de las últimas 1, 3, 12 o 24 horas, o los últimos 7 días.
- Consulta de métricas en la consola de Cloud Eye
  - a. Inicie sesión en la consola de gestión.
  - b. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
  - c. Haga clic en **Service List** y elija **Management & Governance > Cloud Eye**.
  - d. Elija **Cloud Service Monitoring > Elastic IP and Bandwidth**.
  - e. Localice el EIP de una puerta de enlace VPN y haga clic en **View Metric** en la columna **Operation** para ver los datos de supervisión de EIP.


Puede ver los datos de las últimas 1, 3, 12 o 24 horas, o los últimos 7 días.

## 1.7.4 Creación de reglas de alarma

### Escenarios

Puede configurar reglas de alarma en la consola de Cloud Eye para realizar un seguimiento del estado de su VPN 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. Haga clic en **Service List** y elija **Management & Governance > Cloud Eye**.
4. Elija **Cloud Service Monitoring > Virtual Private Network**, busque la conexión VPN de destino y haga clic en **Create Alarm Rule** en la columna **Operation**.

Para VPN, configure las reglas de alarma en la página de pestaña **Dedicated Connections**. Para VPN clásica, configure las reglas de alarma en la página de pestaña **VPN Connections**.

- De forma predeterminada, VPN no proporciona ninguna plantilla de alarma. Debe hacer clic en **Create Custom Template** para crear una plantilla en primer lugar. A continuación, elija **Cloud Service Monitoring > Virtual Private Network** y haga clic en **Create Alarm Rule** para configurar una regla de alarma.
- De forma predeterminada, Classic VPN proporciona una plantilla de alarma llamada **Virtual Private Network Alarm Template**. Puede utilizar esta plantilla predeterminada sin crear una nueva.

Si la política de alarma de la plantilla de alarma predeterminada no cumple con sus requisitos, puede crear una plantilla de alarma personalizada haciendo clic en **Create Custom Template**. A continuación, elija **Cloud Service Monitoring > Virtual Private Network** y haga clic en **Create Alarm Rule** para configurar una regla de alarma.

5. Haga clic en **Create**.

Después de crear la regla de alarma, si ha habilitado **Alarm Notification** y configurado los parámetros requeridos, recibirá notificaciones una vez que se active una alarma.



Para obtener más información acerca de las reglas de alarma de VPN, consulte la [Guía de usuario de Cloud Eye](#).

## 1.8 Operaciones clave registradas por CTS

### 1.8.1 Operaciones de VPN que pueden ser registradas por CTS

**Tabla 1-7** enumera las operaciones de VPN que pueden ser registradas por CTS.

**Tabla 1-7** Operaciones de VPN que pueden ser registradas por CTS

Operación	Tipo de recurso	Nombre del rastro
Creación de una puerta de enlace de cliente	customer-gateway	createCgw
Actualización de una puerta de enlace de cliente	customer-gateway	updateCgw




Operación	Tipo de recurso	Nombre del rastro
Eliminación de una puerta de enlace de cliente	customer-gateway	deleteCgw
Creación de una VPN gateway	vpn-gateway	createVgw
Actualización de una puerta de enlace VPN	vpn-gateway	updateVgw
Eliminación de una puerta de enlace VPN	vpn-gateway	deleteVgw
Creación de una puerta de enlace VPN anual/mensual	vpn-gateway	CreatePrePaidVgw
Actualización del estado de la puerta de enlace VPN	vpn-gateway	UpdateResourceState
Creación de una conexión VPN	vpn-connection	createVpnConnection
Actualización de una conexión VPN	vpn-connection	updateVpnConnection
Eliminación de una conexión de VPN	vpn-connection	deleteVpnConnection

## 1.8.2 Consulta de rastros de CTS

Cuando CTS está habilitado, el sistema inicia las operaciones de registro realizadas en recursos VPN. Puede ver los registros de operación de los últimos siete días en la consola de gestión de CTS.

### Procedimiento

**Paso 1** Inicie sesión en la consola de gestión.

**Paso 2** En el panel de navegación de la izquierda, haga clic en  y elija **Management & Governance > Cloud Trace Service**.


**Paso 3** En el panel de navegación, elija **Trace List**.

**Paso 4** Especifique los criterios de búsqueda según sea necesario.

- Intervalo de tiempo de búsqueda: en la esquina superior derecha, seleccione **Last 1 hour**, **Last 1 day**, o **Last 1 week**, o especifique un intervalo de tiempo personalizado.

- **Trace Type, Trace Source, Resource Type, y Search By:** Seleccione un filtro de la lista desplegable.  
Si selecciona **Resource ID** para **Search By**, especifique un ID de recurso.  
Si selecciona **Data** para **Trace Type**, solo puede filtrar los seguimientos por rastreador.
- **Operator:** Seleccione uno o más operadores de la lista desplegable.
- **Trace Status:** seleccione uno de **All trace statuses, Normal, Warning, y Incident**.

**Paso 5** Haga clic en **Query**.

**Paso 6** Haga clic en  a la izquierda de una traza para ampliar sus detalles.

**Paso 7** Haga clic en **View Trace** en la columna **Operation** para ver el contenido detallado de un rastro.

----Fin

## 1.9 Gestión de permisos

### 1.9.1 Creación de un usuario y concesión de permisos VPN

En este tema se describe cómo usar **IAM** para implementar un control de permisos detallado para sus recursos VPN. 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 VPN.
- Conceda sólo los permisos necesarios para que los usuarios realicen una tarea específica.
- Confíe una cuenta de Huawei Cloud o un servicio en la nube para realizar operaciones profesionales y eficientes en sus recursos VPN.

Si su cuenta de Huawei Cloud no necesita usuarios individuales de IAM, omita este tema.

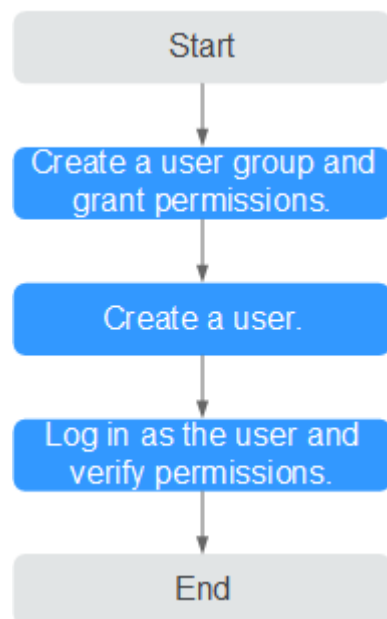
En esta sección se describe el procedimiento para conceder permisos (ver [Figura 1-1](#)).

#### Prerrequisitos

Obtenga información sobre los permisos (consulte [Gestión de permisos](#)) admitidos por VPN y elija políticas o roles en función de sus requisitos. Para obtener los permisos de otros servicios, consulte [Permisos de sistema](#).

## Flujo del proceso

**Figura 1-1** Proceso de concesión de permisos VPN



1. **Crear un grupo de usuarios y asignarle permisos.**  
Cree un grupo de usuarios en la consola de IAM y adjunte la política **VPN Administrator** al grupo.
2. **Crear un usuario de IAM** y agregarlo a un grupo de usuarios.  
Cree un usuario en la consola IAM y agregue el usuario al grupo creado en **1**.
3. **Iniciar sesión** y verificar los permisos.  
Inicie sesión en la consola de gestión como el usuario creado. Cambie a la región autorizada y verifique los permisos.
  - Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **Virtual Private Network**. Haga clic en **Buy VPN Gateway** en la esquina superior derecha. Si la puerta de enlace VPN se ha creado correctamente, la política **VPN Administrator** ya ha entrado en vigor.
  - Elija cualquier otro servicio en **Service List**. Si aparece un mensaje que indica que no tiene permisos suficientes para acceder al servicio, la **VPN Administrator** de VPN ya ha entrado en vigor.

### 1.9.2 Políticas personalizadas de VPN

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de VPN.

Puede crear políticas personalizadas de cualquiera de las siguientes maneras:

- Editor visual: Seleccione servicios en la nube, acciones, recursos y condiciones de solicitud. Esto no requiere conocimiento de la sintaxis de políticas.
- JSON: Editar las políticas JSON desde cero o basándose en una política existente.

Para obtener más información, consulte **Creación de una política personalizada**. La siguiente sección contiene ejemplos de políticas personalizadas de VPN comunes.

## Ejemplo de política personalizada de VPN

- Ejemplo 1: Permitir a los usuarios eliminar puertas de enlace VPN

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpn:vgws:delete"
      ]
    }
  ]
}
```

- Ejemplo 2: Negar a los usuarios que eliminen una conexión VPN

Una política con solo permisos Deny debe usarse junto con otras políticas para que surtan efecto. Si las políticas asignadas 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 **VPN FullAccess** a un usuario, pero también prohibir que el usuario elimine conexiones VPN. Crear una política personalizada para denegar la eliminación de la conexión VPN y asignar ambas políticas al grupo al que pertenece el usuario. Entonces el usuario puede realizar todas las operaciones en VPN excepto eliminar conexiones VPN. A continuación se muestra un ejemplo de una política de denegación:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "vpn:connections:delete"
      ]
    }
  ]
}
```

- Ejemplo 3: definición de varias acciones en una política

Una política personalizada puede contener 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": [
    {
      "Effect": "Allow",
      "Action": [
        "vpn:connections:create",
        "vpn:vpnGateways:create",
        "vpn:cgws:create"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "vpn:connections:delete",
        "vpn:vpnGateways:delete",
        "vpn:cgws:create"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:subnets:get",

```

```
    "vpc:vpcs:list"  
  ]  
}  
}
```

## 1.10 Cuotas

### ¿Qué es una cuota?

Las cuotas pueden limitar el número o la cantidad de recursos disponibles para los usuarios, como el número máximo de ECS o discos EVS que se pueden crear.


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

### Tipos de recursos

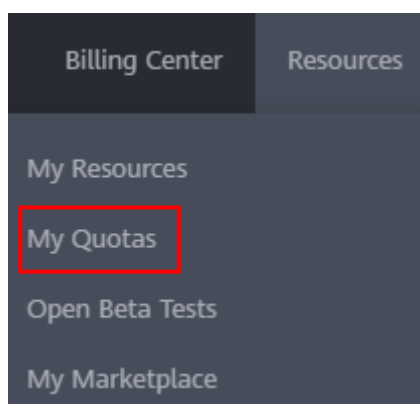
- Los recursos VPN clásicos incluyen puertas de enlace de Classic VPN y conexiones de Classic VPN.
- Los recursos VPN incluyen puertas de enlace de VPN, grupos de conexión VPN y puertas de enlace de clientes.

La cuota total de cada tipo de recurso varía según las regiones.

### ¿Cómo puedo ver mis cuotas?

1. Inicie sesión en la consola de gestión.
2. Haga clic  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En la esquina superior derecha de la página, seleccione **Resources > My Quotas**. Se muestra la página **Service Quota**.

**Figura 1-2** Mis cuotas

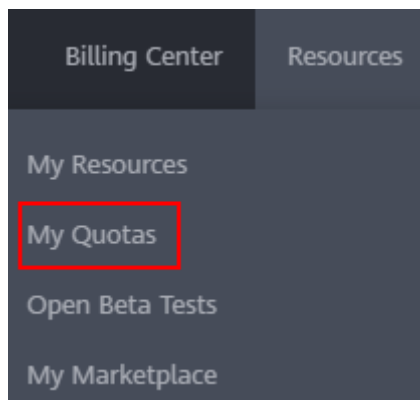


4. Vea la cuota usada y total de cada tipo de recursos en la página mostrada. Si una cuota no puede cumplir con los requisitos de servicio, solicite una cuota más alta.

## ¿Cómo solicito una cuota más alta?

1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la página, seleccione **Resources > My Quotas**.  
Se muestra la página **Service Quota**.

**Figura 1-3** Mis cuotas



3. Haga clic en **Increase Quota**.
4. En la página **Create Service Ticket**, configure los parámetros según sea necesario.  
En el área **Problem Description**, rellene el contenido y el motivo del ajuste.
5. Después de configurar todos los parámetros necesarios, seleccione **I have read and agree to the Tenant Authorization Letter and Privacy Statement** y haga clic en **Submit**.