

NAT Gateway

Guía del usuario

Edición 01
Fecha 2025-02-07



Copyright © Huawei Technologies Co., Ltd. 2025. Todos los derechos reservados.

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

Marcas y permisos



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

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

Aviso

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

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

Índice

1 Gateway de NAT públicos.....	1
1.1 Descripción general del gateway de NAT público.....	1
1.2 Gestión de los gateway de NAT públicos.....	2
1.2.1 Compra de un gateway de NAT público.....	2
1.2.2 Consulta de una puerta de enlace NAT pública.....	5
1.2.3 Modificación de un gateway NAT público.....	5
1.2.4 Eliminación o cancelación de la suscripción de un gateway NAT público.....	7
1.3 Gestión de reglas de SNAT.....	7
1.3.1 Adición de una regla SNAT.....	7
1.3.2 Consulta de una regla SNAT.....	9
1.3.3 Modificación de una regla SNAT.....	10
1.3.4 Eliminación de una regla SNAT.....	10
1.4 Gestión de reglas de DNAT.....	11
1.4.1 Adición de una regla de DNAT.....	11
1.4.2 Consulta de una regla de DNAT.....	14
1.4.3 Modificación de una regla de la DNAT.....	14
1.4.4 Eliminación de una regla de DNAT.....	15
1.4.5 Eliminación de reglas de DNAT por lotes.....	15
1.4.6 Importación y exportación de reglas de DNAT mediante plantillas.....	16
2 Gateway de NAT privados.....	19
2.1 Descripción general del gateway de NAT privado.....	19
2.2 Compra de un gateway de NAT privado.....	23
2.2.1 Compra de un gateway de NAT privado.....	23
2.2.2 Creación de una subred de tránsito y asignación de una dirección IP de tránsito.....	25
2.2.3 Adición de una regla SNAT.....	27
2.2.4 Adición de una regla de DNAT.....	29
2.3 Gestión de los gateway de NAT privados.....	32
2.3.1 Consulta de un gateway de NAT privado.....	32
2.3.2 Modificación de un gateway de NAT privado.....	33
2.3.3 Eliminación de un gateway de NAT privado.....	33
2.4 Gestión de reglas de SNAT.....	34
2.4.1 Consulta de una regla SNAT.....	34
2.4.2 Modificación de una regla SNAT.....	34

2.4.3 Eliminación de una regla SNAT.....	35
2.5 Gestión de reglas de DNAT.....	35
2.5.1 Consulta de una regla de DNAT.....	35
2.5.2 Modificación de una regla de la DNAT.....	36
2.5.3 Eliminación de una regla de DNAT.....	37
2.6 Gestión de direcciones IP de tránsito.....	37
2.6.1 Asignación de una dirección IP de tránsito.....	37
2.6.2 Consulta de una dirección IP de tránsito.....	38
2.6.3 Liberación de una dirección IP de tránsito.....	38
2.7 Acceso a centros de datos locales u otras VPCs.....	39
3 Gestión de etiquetas de gateway de NAT.....	40
4 Monitoreo.....	43
4.1 Métricas admitidas.....	43
4.2 Creación de reglas de alarma.....	47
4.3 Consulta de métricas.....	50
4.4 Consulta de métricas de recursos mediante un gateway de NAT.....	51
5 Auditoría.....	52
5.1 Operaciones de clave registradas por CTS.....	52
5.2 Consulta de trazas.....	53

1 Gateway de NAT públicos

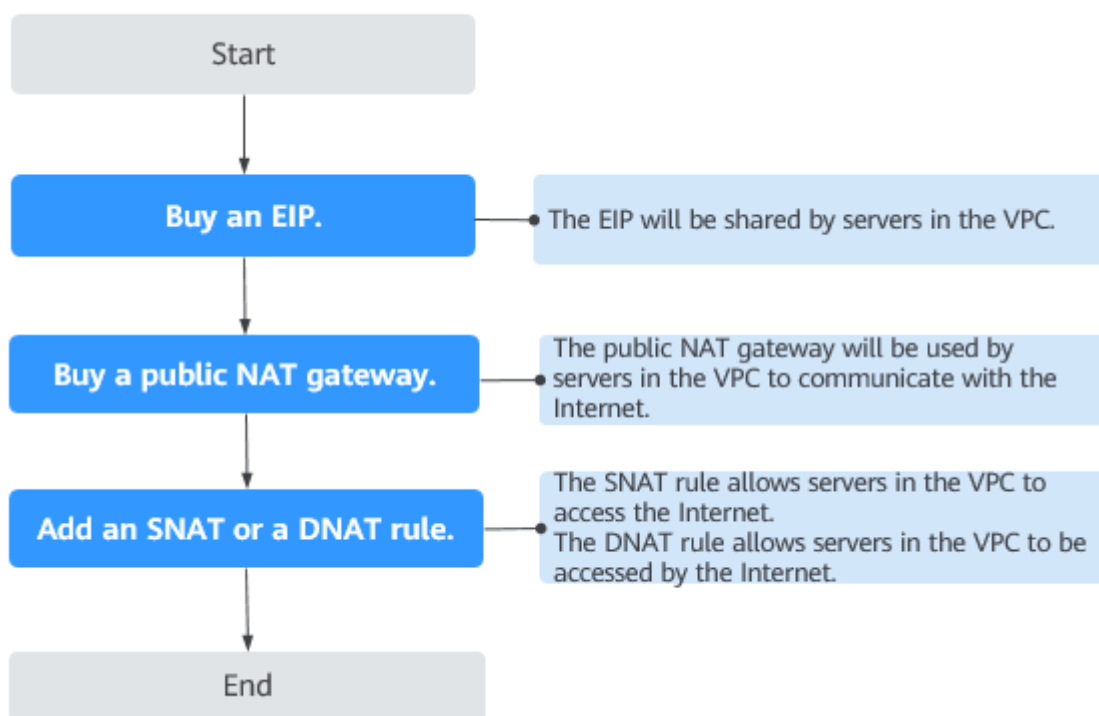
1.1 Descripción general del gateway de NAT público

Los gateways de NAT públicos proporcionan la traducción de direcciones de red con 20 Gbit/s de ancho de banda para los ECS y los BMS en una VPC, o servidores en centros de datos locales que se conectan a una VPC a través de Direct Connect o VPN.

Los gateways de NAT públicos permiten que estos servidores compartan los EIP para acceder a Internet o proporcionar servicios accesibles desde Internet.

El proceso de usar un gateway de NAT público es el siguiente:

Figura 1-1 Proceso de uso de un gateway de NAT público



1.2 Gestión de los gateway de NAT públicos

1.2.1 Compra de un gateway de NAT público

Escenarios

Comprar un gateway de NAT público para permitir que sus servidores accedan a Internet o proporcionen los servicios accesibles desde Internet.

Requisitos previos

- La VPC y la subred donde se desplegará su gateway de NAT público están disponibles.
- Para permitir que el tráfico pase con el gateway de NAT público, se requiere una ruta al gateway de NAT público en la VPC. Cuando crear un gateway de NAT público, una ruta predeterminada 0.0.0.0/0 al gateway de NAT público se agrega automáticamente a la tabla de ruta predeterminada de la VPC. Si la ruta por defecto 0.0.0.0/0 ya existe en la tabla de ruta por defecto de la VPC antes de crear el gateway de NAT público, la ruta por defecto que apunta al gateway de NAT público no se agregará automáticamente. En este caso, realice las siguientes operaciones después de crear correctamente el gateway de NAT público: Agregue manualmente una ruta diferente que apunte al gateway o cree una ruta predeterminada 0.0.0.0/0 que apunte al gateway en la nueva tabla de enrutamiento.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en **Buy Public NAT Gateway**.
5. Configure los parámetros requeridos. Para obtener más información, véase [Tabla 1-1](#).

Tabla 1-1 Descripciones de los parámetros del gateway de NAT público

Parámetro	Descripción
Billing Mode	Los gateway de NAT públicos se facturan de pago por uso.
Region	La región donde se encuentra el gateway NAT público
Name	El nombre del gateway de NAT público Ingrese hasta 64 caracteres. Solo se permiten dígitos, letras, guiones bajos (_) y guiones medios (-).

Parámetro	Descripción
VPC	<p>La VPC a la que pertenece el gateway NAT público</p> <p>La VPC seleccionada no se puede cambiar después de crear el gateway de NAT público.</p> <p>NOTA</p> <p>Para permitir que el tráfico pase con el gateway de NAT público, se requiere una ruta al gateway de NAT público en la VPC. Cuando crear un gateway de NAT público, una ruta predeterminada 0.0.0.0/0 al gateway de NAT público se agrega automáticamente a la tabla de ruta predeterminada de la VPC. Si la ruta por defecto 0.0.0.0/0 ya existe en la tabla de ruta por defecto de la VPC antes de crear el gateway de NAT público, la ruta por defecto que apunta al gateway de NAT público no se agregará automáticamente. En este caso, realice las siguientes operaciones después de crear correctamente el gateway de NAT público: Agregue manualmente una ruta diferente que apunte al gateway o cree una ruta predeterminada 0.0.0.0/0 que apunte al gateway en la nueva tabla de enrutamiento.</p>
Subnet	<p>La subred a la que pertenece el gateway de NAT público</p> <p>La subred debe tener al menos una dirección IP disponible.</p> <p>La subred seleccionada no se puede cambiar después de crear el gateway NAT público.</p>
Specifications	<p>Las especificaciones del gateway de NAT público</p> <p>El valor puede ser Extra-large, Large, Medium o Small. Para ver más detalles sobre las especificaciones, haga clic en Learn more en la página.</p>
Enterprise Project	<p>El proyecto empresarial al que pertenece el gateway de NAT público</p> <p>Si se ha configurado un proyecto de empresa, seleccione el proyecto de empresa. Si no ha configurado ningún proyecto de empresa, seleccione el proyecto de empresa default.</p>
Description	<p>Información complementaria sobre el gateway de NAT público</p> <p>Ingrese hasta 255 caracteres.</p>
Tag	<p>La etiqueta del gateway de NAT público. Una etiqueta es un par de clave-valor.</p> <p>Puede agregar hasta 10 etiquetas a cada gateway NAT público.</p> <p>La clave y el valor de la etiqueta deben cumplir los requisitos de Tabla 1-2.</p>

Tabla 1-2 Tag requirements


Parámetro	Requisito
Key	<ul style="list-style-type: none"> ● No se puede dejar en blanco. ● Debe ser único para cada gateway de NAT. ● Puede contener un máximo de 36 caracteres. ● No puede contener signos iguales (=), asteriscos (*), corchetes angulares izquierdos (<), corchetes angulares rectos (>), barras invertidas (\), comas (,), barras verticales (), y barras (/), y los caracteres primero y último no pueden ser espacios.
Value	<ul style="list-style-type: none"> ● Puede contener un máximo de 43 caracteres. ● No puede contener signos iguales (=), asteriscos (*), corchetes angulares izquierdos (<), corchetes angulares rectos (>), barras invertidas (\), comas (,), barras verticales (), y barras (/), y los caracteres primero y último no pueden ser espacios.

Después de configurar los parámetros, se mostrará el precio del gateway de NAT público. Para ver más detalles de precios, haga clic en **Pricing details** en la página.

- Haga clic en **Submit** para crear un Gateway NAT público.
 Se necesita de 1 a 5 minutos para crear un Gateway NAT público.
- En la lista, vea el estado del Gateway NAT público.

Después de crear el gateway de NAT público, compruebe si existe una ruta predeterminada (0.0.0.0/0) que apunte al gateway de NAT público en la tabla de ruta predeterminada de la VPC donde está el gateway de NAT público. Si no, agregue una ruta que apunte al gateway de NAT público a la tabla de ruta por defecto, alternativamente, cree una tabla de ruta personalizada y agregue la ruta por defecto 0.0.0.0/0 que apunte al gateway de NAT público a la tabla. A continuación se describe cómo agregar una ruta a una tabla de ruta personalizada.

Adición de un punto de ruta predeterminado al Gateway NAT público

- Inicie sesión en la consola de gestión.
- Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
- En **Networking**, seleccione **Virtual Private Cloud**.
- En el panel de navegación de la izquierda, elija **Route Tables**.
- En la página **Route Tables**, haga clic en **Create Route Table** en la esquina superior derecha.

VPC: Seleccione la VPC a la que pertenece el Gateway NAT público.

NOTA

Si la cuota de tabla de ruta personalizada es insuficiente, [cree un ticket de servicio](#) para aumentar la cuota de tabla de ruta.

- Después de crear la tabla de ruta personalizada, haga clic en su nombre.
 Se muestra la página **Summary**.

- Haga clic en **Add Route** y configure los parámetros de la siguiente manera:
Destination: Póngalo en **0.0.0.0/0**.
Next Hop Type: Seleccione **NAT gateway**.
Next Hop: Seleccione el gateway NAT creado.

Figura 1-2 Agregar la ruta

The screenshot shows a modal window titled "Add Route" with a close button (X) in the top right corner. Below the title, it indicates "Route Table rtb-VPC". The main area contains a table with the following columns: "Destination", "Next Hop Type", "Next Hop", and "Description". The "Destination" field contains "0.0.0.0/0", "Next Hop Type" is a dropdown menu set to "NAT gateway", and "Next Hop" is a dropdown menu set to "nat-49ee(8947eef5-6948-4245-af45-...)". There is a trash icon to the right of the "Description" field. Below the table, there is a "+ Add Route" button and two buttons: "OK" (red) and "Cancel" (white).

- Haga clic en **OK**.

1.2.2 Consulta de una puerta de enlace NAT pública


Escenarios

Puede ver información sobre un gateway de NAT público.

Prerrequisitos

Hay un gateway de NAT público disponible.

Procedimiento

- Inicie sesión en la consola de gestión.
- Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
- Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
- En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
- Vea información sobre el gateway de NAT público en la página mostrada.

1.2.3 Modificación de un gateway NAT público

Escenarios

Puede modificar el nombre, el tipo o la descripción de un gateway NAT público.

El uso de un gateway NAT público de un tipo más grande no afecta a los servicios, pero si cambia a un gateway NAT público de un tipo más pequeño, asegúrese de que la capacidad reducida seguirá siendo suficiente para cumplir con sus requisitos de servicio.

Prerrequisitos

Hay un gateway de NAT público disponible.

Procedimiento


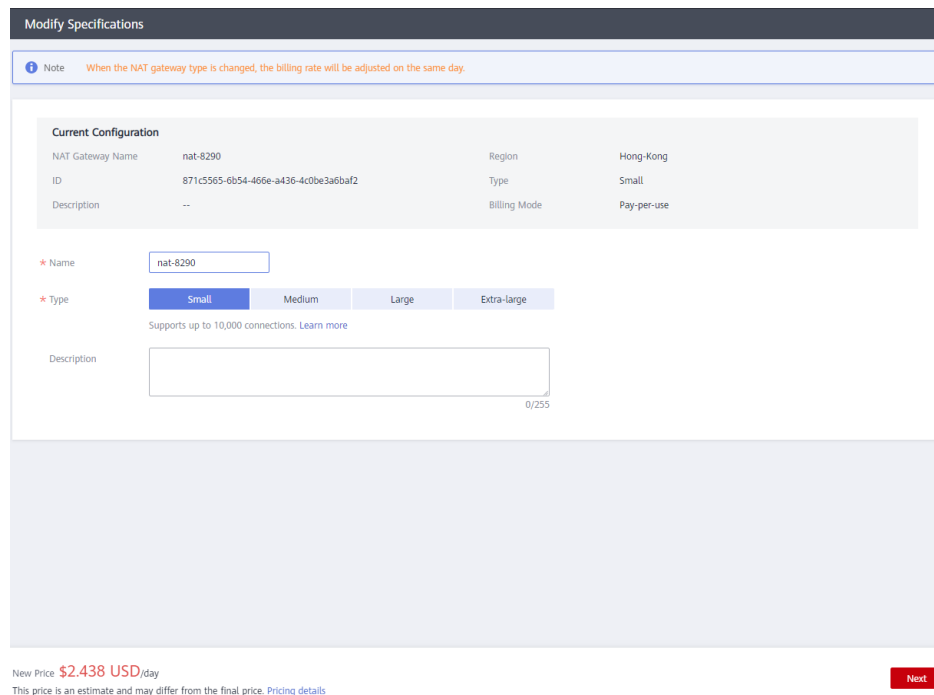
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, busque la fila que contiene la gateway NAT pública que desea modificar y haga clic en **Modify** en la columna **Operation**.
5. Modifique el nombre, tipo o descripción del gateway NAT público según sea necesario.

Figura 1-3 Modificar las especificaciones



6. Haga clic en **OK**.

1.2.4 Eliminación o cancelación de la suscripción de un gateway NAT público

Escenarios

Puede eliminar o cancelar la suscripción de los gateway NAT públicos que ya no son necesarios para liberar recursos y reducir costos.


NOTA

- Para darse de baja de una gateway NAT pública de pago por uso, solo tiene que **eliminar el gateway de NAT**.

Prerrequisitos

Se han eliminado todas las reglas de SNAT y de DNAT creadas en el gateway NAT público.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, busque la fila que contiene el gateway de NAT público que desea eliminar y haga clic en **Delete** en la columna **Operation**.
5. En la caja de diálogo que aparece, haga clic en **Yes**.

1.3 Gestión de reglas de SNAT

1.3.1 Adición de una regla SNAT

Escenarios

Una vez creada la gateway NAT pública, agregue reglas SNAT para que los servidores de una subred de VPC o servidores conectados a una VPC a través de Direct Connect o CC puedan acceder a Internet compartiendo una EIP.

Cada regla SNAT está configurada para una sola subred. Si hay varias subredes en una VPC, puede crear varias reglas SNAT para permitirles compartir EIP.

Prerrequisitos

Hay un gateway de NAT público disponible.

Procedimiento


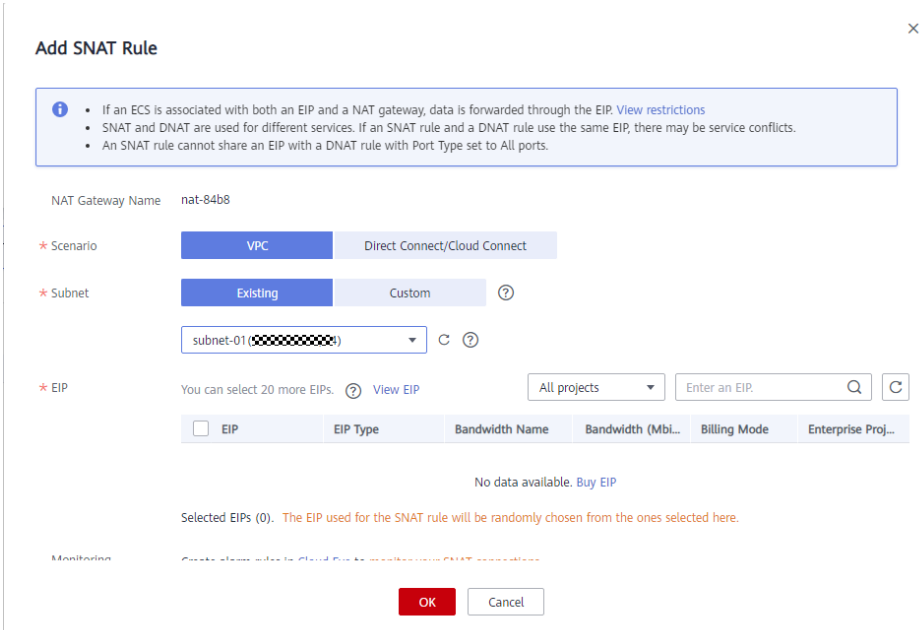
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway NAT público para el que desea agregar una regla SNAT.
5. En la ficha **SNAT Rules**, haga clic en **Add SNAT Rule**.

Figura 1-4 Agregar la regla de SNAT



6. Configure los parámetros requeridos. Para más detalles, consulte [Tabla 1-3](#).

Tabla 1-3 Descripciones de parámetros

Parámetro	Descripción
Scenario	<p>Los escenarios en los que se utiliza la regla de SNAT</p> <p>Seleccione VPC si sus servidores de una VPC necesitan acceder a Internet.</p> <p>Seleccione Direct Connect/Cloud Connect si los servidores que están conectados a una VPC a través de Direct Connect o VPN en su centro de datos necesitan tener acceso a Internet.</p>

Parámetro	Descripción
Subnet	<ul style="list-style-type: none"> ● Existing: seleccione una subred existente para permitir que los servidores de esta subred utilicen la regla SNAT para acceder a Internet. ● Custom: especifique el bloque CIDR en un subconjunto de una subred VPC actual o introduzca una dirección IP del servidor para que el servidor pueda utilizar la regla SNAT para acceder a Internet. <p>NOTA Al seleccionar Custom, puede escribir 0.0.0.0/0. Solo se admite una dirección IP de servidor de 32 bits.</p>
EIP	<p>El EIP utilizado para acceder a Internet</p> <p>Puede seleccionar una EIP que no se ha enlazado, que se ha enlazado a una regla de DNAT con Port Type establecido en Specific port del gateway NAT público actual, o que se ha enlazado a una regla de SNAT del gateway NAT público actual.</p> <p>Puede seleccionar hasta 20 EIPs para una regla SNAT a la vez. Si ha seleccionado varias EIP para una regla de SNAT, se elegirá una EIP de su selección al azar.</p>
Monitoring	<p>Puede crear reglas de alarma en la consola de Cloud Eye para monitorear sus conexiones SNAT y mantenerse informado de cualquier cambio en el momento oportuno.</p>
Description	<p>Información complementaria sobre la regla SNAT</p> <p>Ingrese hasta 255 caracteres.</p>

7. Haga clic en **OK**.

 **NOTA**

- Puede agregar varias reglas de SNAT para un gateway de NAT público para satisfacer sus requisitos de servicio.
- Cada VPC puede asociarse con múltiples gateway de NAT públicos.
- Solo se puede agregar una regla SNAT para cada subred de VPC.

1.3.2 Consulta de una regla SNAT


Escenarios

Después de agregar una regla SNAT, puede ver sus detalles.

Prerrequisitos

Se ha agregado una regla de SNAT.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
5. En la lista de reglas de SNAT, vea los detalles sobre la regla de SNAT.

1.3.3 Modificación de una regla SNAT


Escenarios

Puede modificar las reglas de SNAT según sea necesario.

Prerrequisitos

Se ha agregado una regla de SNAT.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
5. En la ficha **SNAT Rules**, busque la fila que contiene la regla de SNAT que desea modificar.
6. Haga clic en **Modify** en la columna **Operation**.
7. En el cuadro de diálogo mostrado, modifique los parámetros según sea necesario.
8. Haga clic en **OK**.

1.3.4 Eliminación de una regla SNAT

Escenarios

Puede eliminar las reglas SNAT que ya no necesite.

Prerrequisitos

Se ha agregado una regla de SNAT.

Procedimiento


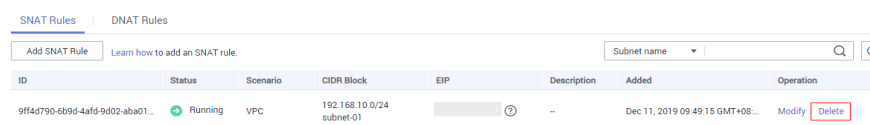
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
5. En la lista de reglas de SNAT, busque la fila que contiene la regla SNAT que desea eliminar y haga clic en **Delete** en la columna **Operation**.

Figura 1-5 Eliminación de una regla SNAT



ID	Status	Scenario	CIDR Block	EIP	Description	Added	Operation
9ff4d790-6b9d-4afd-9d02-aba01...	Running	VPC	192.168.10.0/24 subnet-01		?	Dec 11, 2019 09:49:15 GMT+08:...	Modify Delete

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

1.4 Gestión de reglas de DNAT

1.4.1 Adición de una regla de DNAT

Escenarios


Después de crear un gateway de NAT público, puede agregar las reglas de DNAT para permitir que los servidores de su VPC proporcionen servicios accesibles desde Internet.

Solo puede configurar una regla de DNAT para cada puerto de un servidor. Un puerto puede asignarse a un solo EIP. Si varios servidores necesitan proporcionar servicios accesibles desde Internet, cree varias reglas de DNAT.

Prerrequisitos

Hay un gateway de NAT público disponible.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway NAT público para la que desea agregar una regla de DNAT.

5. En la página de detalles de la gateway NAT pública, haga clic en la ficha **DNAT Rules**.
6. Haga clic en **Add DNAT Rule**.

Figura 1-6 Agregar la regla de DNAT

Add DNAT Rule

Info

- If your ECS has an EIP bound, you do not need to add a DNAT rule. If you do, the forwarded DNAT packets may be interrupted. [View restrictions](#)
- You need to add security group rules to allow inbound or outbound traffic after you add a DNAT rule. [Manage security group rules](#)
- SNAT and DNAT are used for different services. If an SNAT rule and a DNAT rule use the same EIP, there may be service conflicts. An SNAT rule cannot share an EIP with a DNAT rule with Port Type set to All ports.

NAT Gateway Name: nat-1121

* Scenario: **VPC** | Direct Connect/Cloud Connect

* Port Type: **Specific port** | All ports

* Protocol: TCP

* EIP: (5 Mbit/s | Pay-per-use | default) | [View EIP](#)

Bandwidth: 5 Mbit/s | Billing Mode: Pay-per-use
Enterprise Project: default

* Outside Port:

* Private IP Address: | [View ECS IP Address](#)

* Inside Port:

OK | Cancel

7. Configure los parámetros requeridos. Para más detalles, consulte [Tabla 1-4](#).

Tabla 1-4 Descripciones de parámetros

Parámetro	Descripción
Scenario	<p>Seleccione VPC si sus servidores de una VPC usarán la regla de DNAT para compartir el mismo EIP para proporcionar servicios accesibles desde Internet.</p> <p>Direct Connect/Cloud Connect: seleccione este escenario si los servidores de un centro de datos local conectados a una VPC a través de Direct Connect o Cloud Connect utilizarán la regla DNAT para proporcionar servicios accesibles desde Internet.</p>
Port Type	<p>El tipo de puerto</p> <ul style="list-style-type: none"> All ports: Esto es efectivamente como tener una EIP regular unido a sus servidores. Todas las solicitudes recibidas por el gateway serán reenviadas a sus servidores, independientemente del puerto o protocolo utilizado. Specific port: El gateway NAT público reenvía solicitudes a sus servidores solo desde el puerto exterior y al puerto interior configurado aquí, y solo si utilizan el protocolo correcto.

Parámetro	Descripción
Protocol	El protocolo puede ser TCP o UDP. Este parámetro está disponible si selecciona Specific port para Port Type . Si selecciona All ports , este parámetro es All de forma predeterminada.
EIP	El EIP que será utilizado por el servidor para proporcionar servicios accesibles desde Internet Puede seleccionar una EIP que no se ha enlazado, que se ha enlazado a una regla de DNAT con Port Type establecido en Specific port del gateway NAT público actual, o que se ha enlazado a una regla de SNAT del gateway NAT público actual.
Outside Port	El puerto de la EIP Este parámetro sólo está disponible si selecciona Specific port para Port Type . Rango: 1 a 65535 Puede introducir un número de puerto específico o un intervalo de puertos, por ejemplo, 80 o 80-100.
Private IP Address	<ul style="list-style-type: none"> ● En un escenario de VPC, establezca este parámetro en la dirección IP del servidor en una VPC. Esta dirección IP es utilizada por el servidor para proporcionar servicios accesibles desde Internet a través de DNAT. ● En un escenario de Direct Connect, establezca este parámetro en la dirección IP del servidor en su centro de datos local o en su dirección IP privada. Esta dirección IP es utilizada por servidores locales que están conectados a una VPC a través de Direct Connect o Cloud Connect para proporcionar servicios accesibles desde Internet a través de DNAT. <p>NOTA En el escenario Direct Connect o Cloud Connect, la dirección IP privada también puede ser una dirección IP virtual o una dirección IP privada de un balanceador de carga.</p> <ul style="list-style-type: none"> ● Configure el puerto de Private IP Address si selecciona Specific port para Port Type.
Inside Port	El puerto del servidor que utiliza la regla de DNAT para proporcionar servicios accesibles desde Internet Este parámetro sólo está disponible si selecciona Specific port para Port Type . Rango: 1 a 65535 Puede introducir un número de puerto específico o un intervalo de puertos, por ejemplo, 80 o 80-100.
Description	Información complementaria sobre la regla de la DNAT Ingrese hasta 255 caracteres.

8. Haga clic en **OK**.
 Una vez creada la regla, su estado cambia a **Running**.

AVISO

Después de agregar una regla de DNAT, agregue reglas al grupo de seguridad asociado con los servidores para permitir el tráfico entrante o saliente. De lo contrario, la regla de la DNAT no tiene efecto.

1.4.2 Consulta de una regla de DNAT


Escenarios

Después de agregar una regla de DNAT, puede ver sus detalles.

Prerrequisitos

Se ha agregado una regla de DNAT.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
5. En la página de detalles de la gateway NAT pública, haga clic en la ficha **DNAT Rules**.
6. En la lista de reglas de DNAT, vea los detalles sobre la regla de DNAT.

1.4.3 Modificación de una regla de la DNAT


Escenarios

Puede modificar las reglas de la DNAT según sea necesario.

Prerrequisitos

Se ha agregado una regla de DNAT.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.

4. En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
5. En la página de detalles de la gateway NAT pública, haga clic en la ficha **DNAT Rules**.
6. En la lista de reglas de DNAT, busque la fila que contiene la regla de DNAT que desea modificar y haga clic en **Modify** en la columna **Operation**.
7. En el cuadro de diálogo mostrado, modifique los parámetros según sea necesario.
8. Haga clic en **OK**.

1.4.4 Eliminación de una regla de DNAT

Escenarios

Puede eliminar una regla de DNAT que ya no necesite.

Prerrequisitos

Se ha agregado una regla de DNAT.

Procedimiento


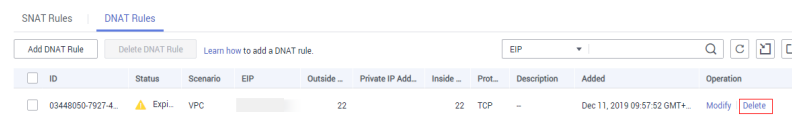

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
5. En la página de detalles de la gateway NAT pública, haga clic en la ficha **DNAT Rules**.
6. En la lista de reglas de DNAT, busque la fila que contiene la regla de DNAT que desea eliminar y haga clic en **Delete** en la columna **Operation**.

Figura 1-7 Eliminación de una regla de DNAT



ID	Status	Scenario	EIP	Outside ...	Private IP Add...	Inside ...	Prot...	Description	Added	Operation
03448050-7927-4...		Epi...	VPC		22	22	TCP	-	Dec 11, 2019 09:57:52 GMT+...	Modify Delete

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

1.4.5 Eliminación de reglas de DNAT por lotes


Escenarios

Puede eliminar las reglas de la DNAT que ya no necesite.

Prerrequisitos

Se han agregado reglas de la DNAT.

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 la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway de NAT público de destino.
5. En la página de detalles de la gateway NAT pública, haga clic en la ficha **DNAT Rules**.
6. En la lista de reglas de DNAT, seleccione las reglas de DNAT de destino y haga clic en **Delete DNAT Rule**.
7. En la caja de diálogo que aparece, haga clic en **Yes**.

1.4.6 Importación y exportación de reglas de DNAT mediante plantillas

Escenarios

Después de crear un gateway de NAT público, puede agregar las reglas de DNAT para permitir que los servidores de su VPC proporcionen servicios accesibles desde Internet.

Se configura una regla de DNAT para un servidor. Si hay varios servidores, cree varias reglas de DNAT.

Prerrequisitos

Hay un gateway de NAT público disponible.

Procedimiento


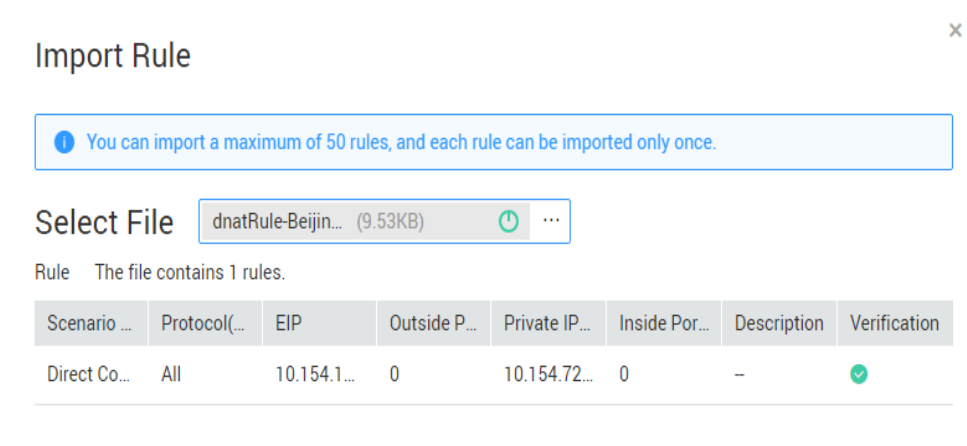
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
Se muestra la página Gateway NAT público.
4. En la página mostrada, haga clic en el nombre del gateway NAT público para la que desea agregar una regla de DNAT.
5. En la página de detalles de la gateway NAT pública, haga clic en la ficha **DNAT Rules**.
6. En la página mostrada, haga clic en **Import Rule** y, a continuación, en **Download Template**.
7. Rellene los parámetros de la regla de la DNAT basados en el encabezado de la tabla en la plantilla. Para más detalles, consulte [Tabla 1-5](#).

Tabla 1-5 Descripciones de parámetros

Parámetro	Descripción
Scenario	<p>Están disponibles los dos escenarios siguientes:</p> <ul style="list-style-type: none"> ● VPC: Los servidores de una VPC pueden compartir un EIP para proporcionar servicios accesibles desde Internet a través de la regla DNAT. ● Direct Connect/Cloud Connect: seleccione este escenario si los servidores de un centro de datos local conectados a una VPC a través de Direct Connect o Cloud Connect utilizarán la regla DNAT para proporcionar servicios accesibles desde Internet.
Protocol	El protocolo puede ser TCP, UDP o All.
EIP	<p>El EIP que será utilizado por el servidor para prestar servicios accesibles desde Internet</p> <p>Sólo los EIP que no se han unido o que se han unido a una regla de DNAT en la VPC actual están disponibles para la selección.</p>
Outside Port	<p>El puerto EIP</p> <p>Este parámetro sólo está disponible si selecciona Specific port para Port Type.</p> <p>Puede introducir un número de puerto específico o un intervalo de puertos, por ejemplo, 80 o 80-100.</p>
Private IP Address	<ul style="list-style-type: none"> ● En un escenario de VPC, establezca este parámetro en la dirección IP del servidor en una VPC. Esta dirección IP es utilizada por el servidor para proporcionar servicios accesibles desde Internet a través de DNAT. ● En un escenario de Direct Connect, establezca este parámetro en la dirección IP del servidor en su centro de datos local o en su dirección IP privada. Esta dirección IP es utilizada por servidores locales que están conectados a una VPC a través de Direct Connect o Cloud Connect para proporcionar servicios accesibles desde Internet a través de DNAT. ● Configure el puerto de dirección IP privada si establece Protocol en TCP o UDP.
Inside Port	<ul style="list-style-type: none"> ● En un escenario de VPC, establezca este parámetro en el puerto del servidor en una VPC. ● En un escenario de Direct Connect, establezca este parámetro en el puerto del servidor en el centro de datos local o en el puerto privado del usuario. ● Este parámetro sólo está disponible si selecciona Specific port para Port Type. <p>La cantidad de puertos internos y la de puertos externos deben coincidir.</p>
Description	Información complementaria sobre la regla de la DNAT. Puede introducir hasta 255 caracteres.

8. Después de rellenar la plantilla, haga clic en **Import Rule**, seleccione la plantilla y haga clic en **Import**.

Figura 1-8 Importar regla



9. Vea los detalles en la lista de reglas de la DNAT.
 Si **Status** está en **Running**, se han agregado las reglas.
10. En la página de la ficha **DNAT Rules**, haga clic en **Export Rule** para exportar la plantilla de regla de DNAT configurada.

2 Gateway de NAT privados

2.1 Descripción general del gateway de NAT privado

Gateway de NAT privados

Los gateway de NAT privados proporcionan servicios de traducción de direcciones privadas para ECS y BMS en una VPC. Puede configurar las reglas de SNAT y DNAT para traducir las direcciones IP de origen y destino en direcciones IP de tránsito, de modo que los servidores de la VPC puedan comunicarse con otras VPC o centros de datos locales.

En especial:

- SNAT permite que varios servidores de AZ en una VPC compartan una dirección IP de tránsito para acceder a centros de datos locales u otras VPC.
- DNAT permite que los servidores que comparten la misma dirección IP de tránsito en una VPC proporcionen servicios accesibles desde centros de datos locales u otras VPC.

Transit Subnet (Subred de tránsito)

Una subred de tránsito funciona como una red de tránsito. Puede configurar una dirección IP de tránsito para la subred de tránsito para que los servidores de una VPC local puedan compartir la dirección IP de tránsito para acceder a centros de datos locales u otras VPC.

Transit VPC (VPC de tránsito)

La VPC de tránsito es la VPC de la que forma parte la subred de tránsito.

Figura 2-1 Gateway de NAT privado

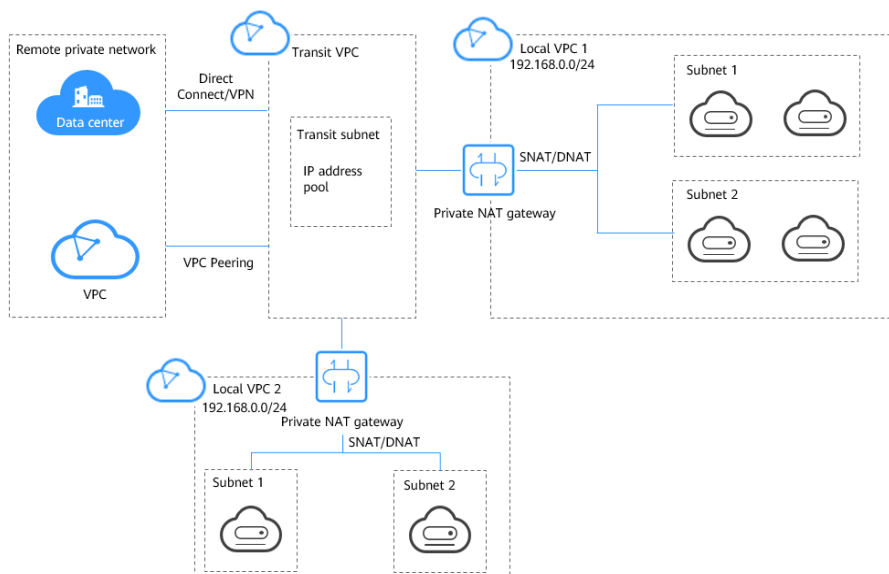


Figura 2-1 muestra dos formas en que se puede implementar un gateway de NAT privado.

- **Comunicaciones entre VPC con bloques CIDR superpuestos**

Normalmente, las VPC con bloques CIDR superpuestos no pueden comunicarse entre sí. Pero con los gateway de NAT privados, puede configurar reglas SNAT y DNAT para traducir las direcciones IP privadas en las VPC para transitar direcciones IP y establecer comunicaciones entre VPC.

- **Usar una dirección IP específica para acceder a una red privada remota**

Un gateway de NAT privado le permite usar una dirección IP específica para acceder a un centro de datos local o a una VPC en una red privada remota. El centro de datos local se conecta a la VPC de tránsito a través de Direct Connect o VPN. La VPC está conectada a la VPC de tránsito a través de una conexión de emparejamiento de VPC. En la figura, la VPC 1 utiliza un gateway de NAT privado para acceder a la red privada remota. Para hacer esto, las reglas SNAT deben configurarse para traducir la dirección IP privada en la VPC 1 en direcciones IP específicas que pueden comunicarse con la red privada, a la izquierda.

NOTA

- Los gateway de NAT privados son gratis por tiempo limitado en las siguientes regiones: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg, and LA-Mexico City2.
- Los gateway de NAT privados se facturan en las siguientes regiones: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok y AP-Singapore.

Ventajas

- **Planificación de red más fácil**

Después de migrar algunas de sus cargas de trabajo desde los centros de datos locales a la nube, una empresa puede querer conservar sus comunicaciones de red internas sin cambios. Los gateway de NAT privados pueden traducir las direcciones IP de sus servidores en la nube a direcciones IP de tránsito en la VPC de tránsito. De esta manera, los servidores pueden comunicarse con centros de datos locales u otras VPC. La empresa

no tiene que reconstruir ninguno de sus servicios y la planificación de la red es mucho más simple.

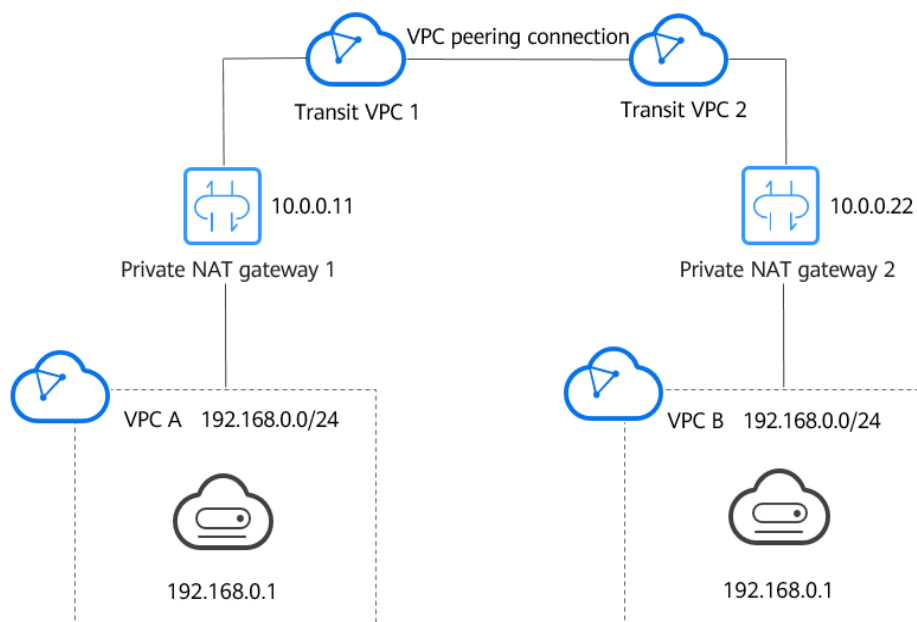
- Cero conflictos de IP
 Dos gateway de NAT privados pueden traducir direcciones IP de dos VPC con un bloque CIDR superpuesto a dos direcciones IP de tránsito, de modo que los servidores en las dos VPC pueden usar las direcciones IP de tránsito para comunicarse entre sí.
- Seguridad fuerte
 Un gateway de NAT privado puede asignar direcciones IP privadas a direcciones IP especificadas por los requisitos de seguridad de la empresa. De esta manera, las empresas pueden elegir qué direcciones IP se utilizan para acceder a diferentes agencias, lo que puede mejorar la seguridad.

Escenarios

- Conexión de VPC con bloques CIDR superpuestos
 Puede configurar dos gateway de NAT privados para dos VPC con bloques CIDR superpuestos y, a continuación, agregar reglas SNAT y DNAT en los dos gateway de NAT privados para permitir que los servidores en las dos VPC usen las direcciones IP de tránsito para comunicarse entre sí.

En la siguiente figura, hay dos VPCs de tránsito y dos gateway de NAT privados. La dirección 192.168.0.1 en la VPC A se traduce a 10.0.0.11, y la dirección IP 192.168.0.1 en la VPC B se traduce a 10.0.0.22. Entonces se puede establecer un interconexión de VPC entre las dos VPC de tránsito para permitir la comunicación entre ellas.

Figura 2-2 Conexión de VPC con bloques CIDR superpuestos

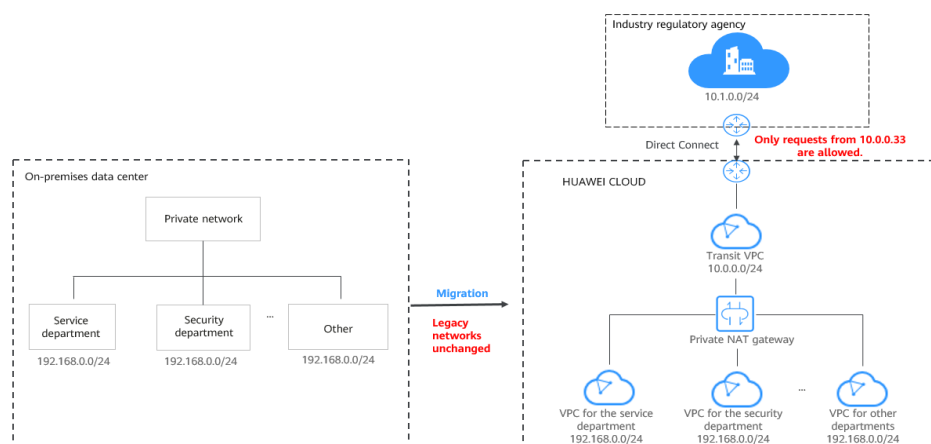


- Migrar cargas de trabajo a la nube sin cambiar la topología de la red ni acceder a las agencias reguladoras desde direcciones IP específicas
 Es posible que las organizaciones quieran migrar sus cargas de trabajo a la nube sin realizar ningún cambio en su topología de red existente. También pueden tener que

acceder a las agencias reguladoras desde direcciones IP específicas según lo requieran estas agencias. Un gateway de NAT privado es una buena opción.

La siguiente figura representa una red de empresa donde las subredes de diferentes departamentos se superponen. Un gateway de NAT privado permite a la empresa mantener la topología de red existente sin cambios mientras migra sus cargas de trabajo a la nube. En este ejemplo, el gateway de NAT privado asigna la dirección IP de cada departamento a 10.0.0.33 para que cada departamento pueda usar 10.0.0.33 para acceder de forma segura a la delegación reguladora.

Figura 2-3 Migrar cargas de trabajo a la nube sin cambiar la topología de la red ni acceder a las agencias reguladoras desde direcciones IP específicas



Diferencias entre los gateway de NAT públicos y privados

Los gateway de NAT públicos usan reglas de SNAT para asignar direcciones IP privadas a EIP, de modo que los servidores de una VPC puedan compartir una EIP para acceder a Internet. Las reglas de la DNAT permiten a los servidores compartir una EIP para proporcionar servicios accesibles desde Internet.

Los gateway de NAT privados usan reglas SNAT para asignar direcciones IP privadas a direcciones IP de tránsito, de modo que los servidores de una VPC puedan acceder a centros de datos locales u otras VPC. Las reglas de DNAT permiten a los servidores compartir la dirección IP de tránsito para proporcionar servicios accesibles desde la red privada.

Tabla 2-1 describe las diferencias entre los gateway de NAT públicos y privados.

Tabla 2-1 Diferencias entre los gateways de NAT públicos y privados

Concepto	Gateway de NAT público	Gateway de NAT privado
Function	Conecta una red privada a Internet	Conecta la red privada entre sí
SNAT	Permite el acceso a Internet	Permite el acceso a centros de datos locales u otras VPCs

Concepto	Gateway de NAT público	Gateway de NAT privado
DNAT	Permite que los servidores proporcionen servicios accesibles desde Internet	Permite que los servidores proporcionen servicios accesibles desde centros de datos locales u otras VPCs en las redes privadas
Communications media	EIP	Dirección IP de tránsito

Enlaces útiles

[Uso de gateway NAT privados para habilitar las comunicaciones entre la nube y las redes locales](#)

2.2 Compra de un gateway de NAT privado

2.2.1 Compra de un gateway de NAT privado

Escenarios

Puede comprar un gateway NAT privado para permitir que los servidores de su VPC accedan o proporcionen servicios accesibles desde centros de datos locales y otras VPC.


NOTA

- Los gateway de NAT privados son gratis por tiempo limitado en las siguientes regiones: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg, and LA-Mexico City2.
- Los gateway de NAT privados se facturan en las siguientes regiones: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok y AP-Singapore.

ATENCIÓN

Al comprar un gateway de NAT privado, debe especificar su VPC, subred y tipo.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.

5. En la página mostrada, haga clic en **Buy Private NAT Gateway**.
6. Configure los parámetros requeridos. Para más detalles, consulte [Tabla 2-2](#).

Tabla 2-2 Descripciones de parámetros

Parámetro	Descripciones de parámetros
Billing Mode	Los gateway de NAT privados se facturan sobre una base de pago por uso.
Region	La región donde se encuentran los gateway de NAT privados
Name	El nombre de los gateway de NAT privados Ingrese hasta 64 caracteres. Solo se permiten dígitos, letras, guiones bajos (_) y guiones (-).
VPC	La VPC a la que pertenecen los gateway de NAT privados La VPC seleccionada no se puede cambiar después del gateway de NAT privado es comprado.
Subnet	La subred de la VPC a la que pertenecen los gateway de NAT privados La subred debe tener al menos una dirección IP disponible. La subred seleccionada no se puede cambiar después de los gateway de NAT privados son comprados.
Type	El tipo de los gateway de NAT privados Hay disponibles cuatro tipos de los gateway de NAT privados: Small , Medium , Large , y Extra-large . Para obtener más información acerca de los tipos, consulte Tipos de los gateway de NAT .
Enterprise Project	El proyecto empresarial al que pertenecen los gateway de NAT privados Si se configura un proyecto de empresa para los gateway de NAT privados, se pertenecen a este proyecto de empresa. Si no especifica un proyecto de empresa, se utilizará el proyecto de empresa default .
Description	Información complementaria sobre los gateway de NAT privados Ingrese hasta 255 caracteres.

7. Haga clic en **Buy Now**.

Enlaces útiles

[Gestión de los gateway de NAT privados](#)

2.2.2 Creación de una subred de tránsito y asignación de una dirección IP de tránsito

Escenarios

Después de crear un gateway NAT privado, cree una subred de tránsito y asigne una dirección IP de tránsito, de modo que los servidores de su VPC puedan compartir la dirección IP de tránsito para acceder o proporcionar servicios accesibles desde centros de datos locales u otras VPC.

Prerrequisitos

- Se ha creado una VPC de tránsito.
- Se ha creado una conexión Direct Connect con el bloque CIDR de VPC **0.0.0.0/0** configurado.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. Haga clic en la ficha **Transit Subnets** y, a continuación, en **Create Transit Subnet**.
6. Configure los parámetros requeridos. Para más detalles, consulte [Tabla 2-3](#).

Figura 2-4 Crear la subred de tránsito

Tabla 2-3 Descripciones de parámetros

Parámetro	Descripción
Name	(Obligatorio) El nombre de la subred de tránsito Ingrese hasta 64 caracteres. Solo se permiten dígitos, letras, guiones bajos (_) y guiones (-).
VPC	(Opcional) La VPC de la que forma parte la subred de tránsito
Subnet	(Opcional) La subred de la que forma parte la subred de tránsito
Description	(Opcional) Información complementaria sobre la subred de tránsito Ingrese hasta 255 caracteres.

7. Haga clic en **OK**.
8. Haga clic en el nombre de la subred de tránsito recién creada.
 Se muestra la página de detalles de la subred de tránsito.
9. Haga clic en **Assign Transit IP Address** y configure los parámetros necesarios.

Figura 2-5 Asignar dirección IP de tránsito

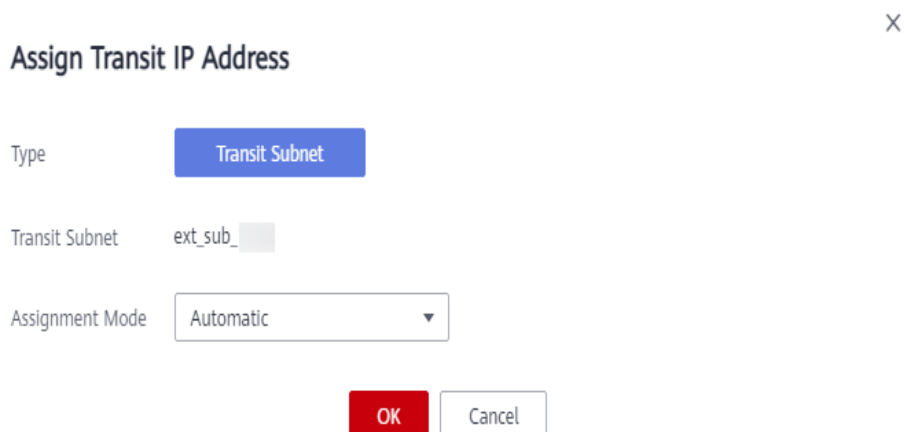


Tabla 2-4 Descripciones de parámetros

Parámetro	Descripción
Assignment Mode	Especifica cómo se asigna la dirección IP de tránsito. Los modos posibles son: <ul style="list-style-type: none"> ● Automático ● Manual
IP Address	Este parámetro sólo está disponible cuando se establezca Assignment Mode en Manual . Esta dirección IP debe formar parte de la subred de tránsito.

10. Haga clic en **OK**.

2.2.3 Adición de una regla SNAT

Escenarios

Después de crear el gateway de NAT privado, agregue reglas SNAT, de modo que algunos o todos los servidores de una subred de VPC puedan compartir una dirección IP de tránsito para acceder a centros de datos locales u otras VPC.

Cada regla SNAT está configurada para una subred. Si hay varias subredes en una VPC, puede agregar varias reglas SNAT para permitirles compartir direcciones IP de tránsito.

Prerrequisitos

- Hay un gateway de NAT privado disponible.
- Tres son las subredes de tránsito y las direcciones IP de tránsito disponibles.
- Se ha creado una conexión Direct Connect con el bloque CIDR de VPC **0.0.0.0/0** configurado.

Procedimiento


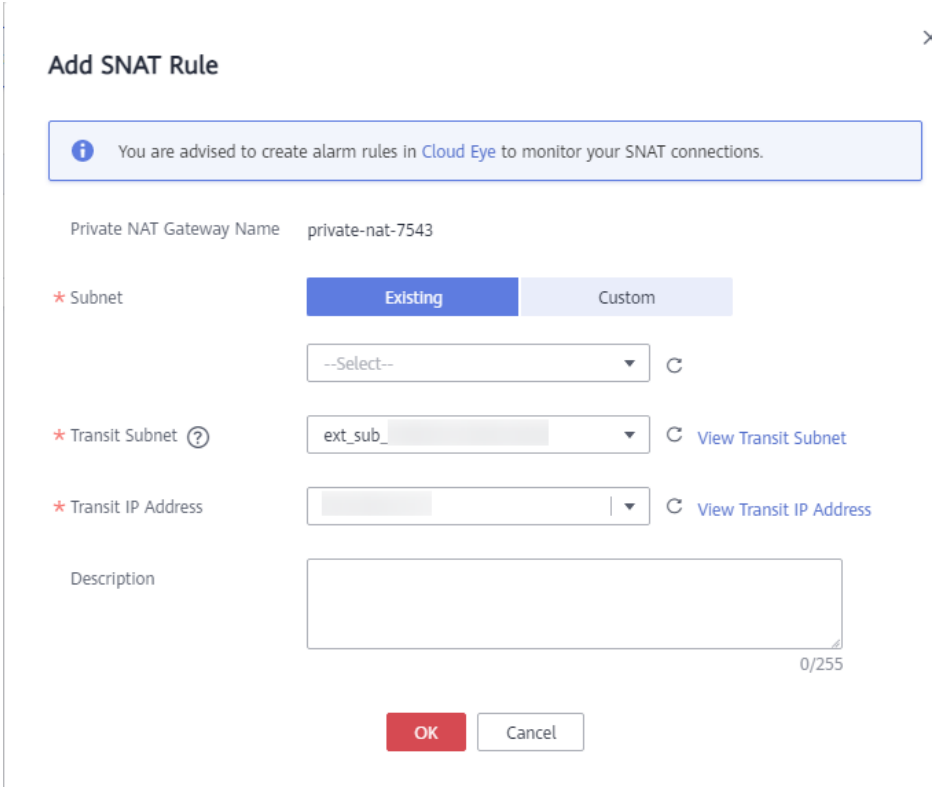
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway de NAT privado para el que desea agregar una regla SNAT.
6. En la ficha **SNAT Rules**, haga clic en **Add SNAT Rule**.
7. Configure los parámetros requeridos. Para más detalles, consulte [Tabla 2-5](#).

Figura 2-6 Agregar la regla de SNAT



Add SNAT Rule ×

i You are advised to create alarm rules in [Cloud Eye](#) to monitor your SNAT connections.

Private NAT Gateway Name private-nat-7543

* Subnet Existing Custom

--Select-- ↻

* Transit Subnet ? ext_sub_ ↕ ↻ [View Transit Subnet](#)

* Transit IP Address | ↕ ↻ [View Transit IP Address](#)

Description 0/255

OK Cancel

Tabla 2-5 Descripciones de parámetros

Parámetro	Descripción
Subnet	<p>Puede establecerlo en Existing o Custom.</p> <ul style="list-style-type: none"> ● Seleccione Existing para aplicar la regla SNAT a una subred existente. ● Seleccione Custom para introducir la subred manualmente. Al seleccionar Custom, puede introducir las direcciones IP de las conexiones Direct Connect.
Transit Subnet	<p>Seleccione la subred de tránsito creada en la VPC de tránsito.</p>
Transit IP Address	<p>La dirección IP de tránsito utilizada para acceder a los centros de datos locales u otras VPCs</p> <p>Puede seleccionar una dirección IP de tránsito que no esté vinculada a ningún recurso o que esté vinculada a una regla SNAT del gateway de NAT privado actual.</p>
Description	<p>Información complementaria sobre la regla SNAT</p> <p>Ingrese hasta 255 caracteres.</p>

- Haga clic en **OK**.

 **NOTA**

Puede agregar varias reglas SNAT para un gateway de NAT privado para satisfacer sus requisitos de servicio.

Enlaces útiles

[Gestión de reglas de SNAT](#)

2.2.4 Adición de una regla de DNAT

Escenarios


Después de crear un gateway NAT privado, puede agregar reglas de DNAT para permitir que los servidores de su VPC proporcionen servicios accesibles desde servidores locales u otras VPC.

Es necesario configurar una regla de DNAT para cada puerto en un servidor que necesita ser accesible. Si varios puertos en un servidor o varios servidores necesitan proporcionar servicios accesibles desde servidores locales u otras VPC, es necesario configurar varias reglas de DNAT.

Prerrequisitos

- Hay un gateway de NAT privado disponible.
- Tres son las subredes de tránsito y las direcciones IP de tránsito disponibles.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway NAT privado para la que desea agregar una regla de DNAT.
6. En la página de detalles del gateway de NAT privado, haga clic en la ficha **DNAT Rules**.
7. Haga clic en **Add DNAT Rule**.

AVISO

Después de agregar una regla de DNAT, agregue reglas al grupo de seguridad asociado con los servidores para permitir el tráfico entrante o saliente. De lo contrario, la regla de la DNAT no tiene efecto.

8. Configure los parámetros requeridos. Para más detalles, consulte [Tabla 2-6](#).

Figura 2-7 Agregar la regla de DNAT

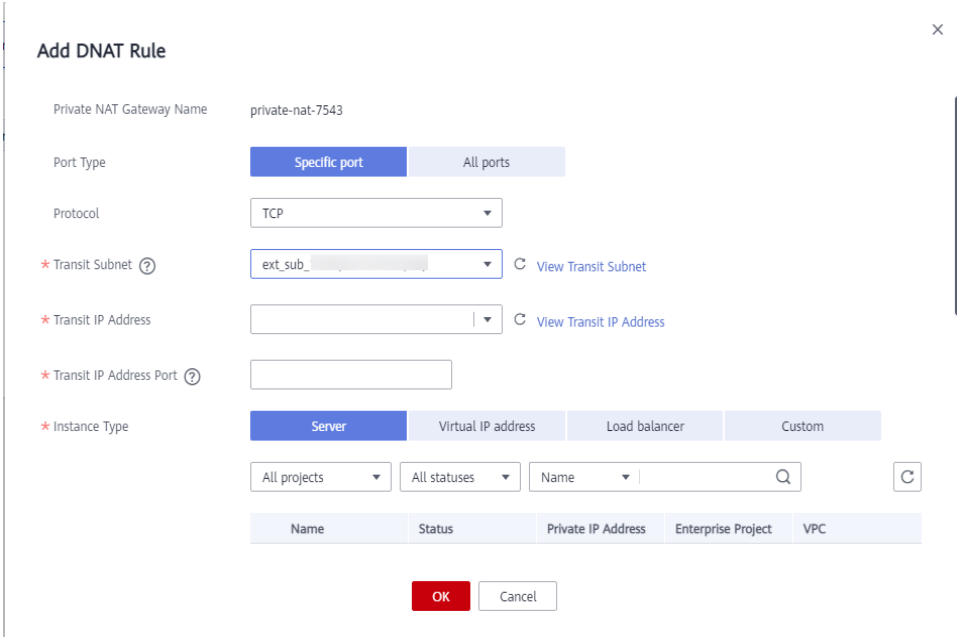


Tabla 2-6 Descripciones de parámetros

Parámetro	Descripción
Port Type	<p>El tipo de puerto</p> <p>El tipo puede ser:</p> <ul style="list-style-type: none"> ● Specific port: El gateway NAT privado reenvía solicitudes a sus servidores solo desde el puerto externo y al puerto interno configurado aquí, y solo si utilizan el protocolo correcto. ● All ports: Esto es efectivamente como tener una dirección IP de tránsito vinculada a sus servidores. Todas las solicitudes recibidas por el gateway serán reenviadas a sus servidores, independientemente del puerto o protocolo utilizado.
Protocol	<p>El protocolo puede ser TCP o UDP</p> <p>Si selecciona All ports, este parámetro es All de forma predeterminada.</p> <p>Este parámetro sólo está disponible si selecciona Specific port para Port Type.</p>
Transit Subnet	<p>Seleccione la subred de tránsito creada en la VPC de tránsito.</p>
Transit IP Address	<p>La dirección IP de tránsito utilizada para acceder a los centros de datos locales u otras VPCs</p> <p>Puede seleccionar una dirección IP de tránsito que no esté enlazada a ningún recurso, o que haya sido enlazada a una regla de DNAT para el gateway NAT privado actual donde Port Type se establece en Specific port.</p>
Transit IP Address Port	<p>El puerto de la dirección IP de tránsito</p> <p>Rango: 1 a 65535</p> <p>Este parámetro sólo está disponible si selecciona Specific port para Port Type.</p>
Instance Type	<p>El tipo de instancia que proporcionará servicios accesibles desde centros de datos locales u otras VPC</p> <p>Los tipos posibles son:</p> <ul style="list-style-type: none"> ● Server ● Virtual IP address ● Load balancer ● Custom
NIC	<p>NIC del servidor</p> <p>Este parámetro está disponible si establece Instance Type en Server.</p>
IP Address	<p>La dirección IP del servidor que presta servicios accesibles desde los centros de datos locales u otras VPC. Este parámetro sólo está disponible si establece Instance Type en Custom.</p>

Parámetro	Descripción
Internal Port	El puerto de la instancia Rango: 1 a 65535 Este parámetro sólo está disponible si selecciona Specific port para Port Type .
Description	Información complementaria sobre la regla de la DNAT Ingrese hasta 255 caracteres.

- Haga clic en **OK**.
 Una vez creada la regla, su estado cambia a **Running**.

Enlaces útiles

[Gestión de reglas de DNAT](#)

2.3 Gestión de los gateway de NAT privados

2.3.1 Consulta de un gateway de NAT privado


Escenarios

Puede ver información sobre un gateway de NAT privado.

Prerrequisitos

Hay un gateway de NAT privado disponible.

Procedimiento

- Inicie sesión en la consola de gestión.
- Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
- Haga clic en **Service List** en la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
 Se muestra la consola de gateway NAT.
- En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
- En la página mostrada, haga clic en el nombre del gateway de NAT privado.
- Vea información sobre el gateway de NAT privado en la página mostrada.

2.3.2 Modificación de un gateway de NAT privado


Escenarios

Puede modificar el nombre, tipo o descripción de un gateway de NAT privado.

Prerrequisitos

Hay un gateway de NAT privado disponible.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, busque la fila que contiene el gateway de NAT privado que desea modificar y haga clic en **Modify** en la columna **Operation**.
6. Modifique el nombre, tipo o descripción del gateway de NAT privado según sea necesario.
7. Confirme su modificación y haga clic en **OK**.
Puede ver información sobre el gateway de NAT modificado en la lista de gateway de NAT privado.

2.3.3 Eliminación de un gateway de NAT privado


Escenarios

Puede eliminar los gateway de NAT privados que ya no son necesarias para liberar recursos y reducir costos.

Prerrequisitos

Se han eliminado todas las reglas SNAT y DNAT creadas en el gateway de NAT privado.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.

4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, busque la fila que contiene la gateway NAT privada que desea eliminar y haga clic en **Delete** en la columna **Operation**.
6. En la caja de diálogo que aparece, haga clic en **Yes**.

2.4 Gestión de reglas de SNAT

2.4.1 Consulta de una regla SNAT


Escenarios

Después de agregar una regla SNAT, puede ver sus detalles.

Prerrequisitos

Se ha agregado una regla de SNAT.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway de NAT privado.
6. En la lista de reglas de SNAT, vea los detalles sobre la regla de SNAT.

2.4.2 Modificación de una regla SNAT


Escenarios

Puede modificar una regla SNAT según sea necesario.

Prerrequisitos

Se ha agregado una regla de SNAT.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway de NAT privado.
6. En la ficha **SNAT Rules**, busque la fila que contiene la regla de SNAT que desea modificar.
7. Haga clic en **Modify** en la columna **Operation**.
8. En el cuadro de diálogo mostrado, modifique los parámetros según sea necesario.
9. Haga clic en **OK**.

2.4.3 Eliminación de una regla SNAT


Escenarios

Puede eliminar las reglas SNAT que ya no necesite.

Prerrequisitos

Se ha agregado una regla de SNAT.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway de NAT privado.
6. En la lista de reglas de SNAT, busque la fila que contiene la regla SNAT que desea eliminar y haga clic en **Delete** en la columna **Operation**.
7. En la caja de diálogo que aparece, haga clic en **Yes**.

2.5 Gestión de reglas de DNAT

2.5.1 Consulta de una regla de DNAT


Escenarios

Después de agregar una regla de DNAT, puede ver sus detalles.

Prerrequisitos

Se ha agregado una regla de DNAT.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway de NAT privado.
6. En la página de detalles del gateway de NAT privado, haga clic en la ficha **DNAT Rules**.
7. En la lista de reglas de DNAT, vea los detalles sobre la regla de DNAT.

2.5.2 Modificación de una regla de la DNAT


Escenarios

Puede modificar una regla de la DNAT según sea necesario.

Prerrequisitos

Se ha agregado una regla de DNAT.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway de NAT privado.
6. En la página de detalles del gateway de NAT privado, haga clic en la ficha **DNAT Rules**.
7. En la lista de reglas de DNAT, busque la fila que contiene la regla de DNAT que desea modificar y haga clic en **Modify** en la columna **Operation**.
8. En el cuadro de diálogo mostrado, modifique los parámetros según sea necesario.
9. Haga clic en **OK**.

2.5.3 Eliminación de una regla de DNAT


Escenarios

Puede eliminar una regla de DNAT que ya no necesite.

Prerrequisitos

Se ha agregado una regla de DNAT.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. En la página mostrada, haga clic en el nombre del gateway de NAT privado.
6. En la página de detalles del gateway de NAT privado, haga clic en la ficha **DNAT Rules**.
7. En la lista de reglas de DNAT, busque la fila que contiene la regla de DNAT que desea eliminar y haga clic en **Delete** en la columna **Operation**.
8. En la caja de diálogo que aparece, haga clic en **Yes**.


2.6 Gestión de direcciones IP de tránsito

2.6.1 Asignación de una dirección IP de tránsito

Escenarios

Todos los servidores de una VPC utilizan la misma dirección IP de tránsito en la subred de tránsito para acceder o proporcionar servicios accesibles desde centros de datos locales u otras 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. Haga clic en **Service List** en la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.

- Haga clic en la ficha **Transit Subnets** y, a continuación, haga clic en el nombre de subred de tránsito de destino.
Se muestra la página de detalles de la subred de tránsito.
- Haga clic en **Assign Transit IP Address** y configure los parámetros necesarios.

Tabla 2-7 Descripciones de parámetros


Parámetro	Descripción
Assignment Mode	Cómo se asigna la dirección IP de tránsito. Los modos posibles son: <ul style="list-style-type: none"> ● Automatic ● Manual
IP Address	Este parámetro sólo está disponible cuando se establece Assignment Mode en Manual . Esta dirección IP debe formar parte de la subred de tránsito.

2.6.2 Consulta de una dirección IP de tránsito

Escenarios

Puede ver detalles acerca de las direcciones IP de tránsito asignadas a usted.

Procedimiento


- Inicie sesión en la consola de gestión.
- Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
- Haga clic en **Service List** en la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
- En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
- Haga clic en la ficha **Transit Subnets** y, a continuación, haga clic en el nombre de subred de tránsito de destino.
Se muestra la página de detalles de la subred de tránsito.
- En el área **Transit IP Addresses**, vea detalles sobre las direcciones IP de tránsito asignadas.

2.6.3 Liberación de una dirección IP de tránsito

Escenarios

Puede liberar una dirección IP de tránsito si ya no la necesita.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
Se muestra la consola de gateway NAT.
4. En el panel de navegación de la izquierda, elija **NAT Gateway > Private NAT Gateway**.
5. Haga clic en la ficha **Transit Subnets** y, a continuación, haga clic en el nombre de subred de tránsito de destino.
Se muestra la página de detalles de la subred de tránsito.
6. En el área **Transit IP Addresses**, localice la dirección IP de tránsito que desea liberar y haga clic en **Release** en la columna **Operation**.
7. Haga clic en **Yes**.

NOTA

Si una dirección IP de tránsito se ha asociado con una regla SNAT o DNAT, no se puede liberar. Para liberar dicha dirección IP de tránsito, elimine primero todas las reglas asociadas a ella.

2.7 Acceso a centros de datos locales u otras VPCs

Acceso a los centros de datos locales

Puede usar Direct Connect o VPN para conectar la VPC de tránsito a sus centros de datos locales.

Para una conexión de mayor calidad, utilice Direct Connect. Para obtener más información, consulte la [Descripción general](#).

Para una conectividad más rentable, use VPN. Para obtener más información, consulte la [Overview](#).

Acceso a otras VPC

Puede utilizar la interconexión de VPC para conectar la VPC de tránsito a otras VPC.

Para obtener más información, consulte la [Descripción general de la interconexión de VPC](#).

3 Gestión de etiquetas de gateway de NAT

Escenarios

Una etiqueta de gateway NAT identifica el gateway NAT. Las etiquetas se pueden agregar a los gateway de NAT para facilitar la identificación y gestión del gateway NAT. Puede agregar una etiqueta a un gateway de NAT al crearlo. Alternativamente, puede agregar una etiqueta a un gateway NAT creado en la página de detalles del gateway NAT. Se puede agregar un máximo de diez etiquetas a cada gateway NAT.

 **NOTA**

Solo los gateway de NAT públicos admiten la gestión de etiquetas.

Una etiqueta consiste en un par clave y valor. [Tabla 3-1](#) enumera los requisitos de valor y clave de etiqueta.

Tabla 3-1 Tag requirements


Parámetro	Requisito
Key	<ul style="list-style-type: none"> ● No se puede dejar en blanco. ● Debe ser único para cada gateway de NAT. ● Puede contener un máximo de 36 caracteres. ● No puede contener signos iguales (=), asteriscos (*), corchetes angulares izquierdos (<), corchetes angulares rectos (>), barras invertidas (\), comas (,), barras verticales (), y barras (/), y los caracteres primero y último no pueden ser espacios.
Value	<ul style="list-style-type: none"> ● Puede contener un máximo de 43 caracteres. ● No puede contener signos iguales (=), asteriscos (*), corchetes angulares izquierdos (<), corchetes angulares rectos (>), barras invertidas (\), comas (,), barras verticales (), y barras (/), y los caracteres primero y último no pueden ser espacios.

Procedimiento

Busque los gateway de NAT públicos por clave de etiqueta o valor de etiqueta en la página que enumera los gateway de NAT públicos.

1. Inicie sesión en la consola de gestión.
2. Haga clic en **Service List** en la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
3. En la esquina superior derecha de la lista de los gateway de NAT públicos, haga clic en **Search by Tag**.
4. En el área mostrada, introduzca la clave de etiqueta y el valor de etiqueta del gateway NAT público que está buscando. Se deben especificar tanto la clave de etiqueta como el valor.
5. Haga clic en + para especificar claves y valores de etiqueta adicionales.
Puede agregar un máximo de diez etiquetas para refinar los resultados de búsqueda. Si agrega más de una etiqueta para buscar los gateway de NAT públicos, las etiquetas se unen automáticamente con AND.
6. Haga clic en **Search**.
El sistema muestra los gateway de NAT públicos que está buscando en función de las claves de etiqueta y los valores de etiqueta introducidos.

Agregar, eliminar, editar y ver etiquetas de un gateway de NAT público en la ficha **Tags**.

1. Inicie sesión en la consola de gestión.
 2. Haga clic en **Service List** en la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.
 3. En la lista de gateway de NAT público, localice el gateway de NAT público cuyas etiquetas desea gestionar y haga clic en su nombre.
Se muestra la página que muestra detalles sobre el gateway de NAT público.
 4. Haga clic en la ficha **Tags** y realice las operaciones deseadas en las etiquetas.
 - Ver una etiqueta.
En la ficha **Tags**, puede ver los detalles de las etiquetas del gateway de NAT público actual, incluido el número de etiquetas y la clave y el valor de cada etiqueta.
 - Agregar una etiqueta.
Haga clic en **Add Tag** en la esquina superior izquierda. En el cuadro de diálogo que se muestra, escriba la clave y el valor de la etiqueta que se va a agregar y haga clic en **OK**.
-  **NOTA**
- Puede utilizar las etiquetas predefinidas según se le solicite para simplificar las operaciones de adición de etiquetas. Para obtener más información, consulte [Etiquetas predefinidas](#).
- Modificar una etiqueta.
Busque la fila que contiene la etiqueta que se va a 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**.
 - Eliminar una etiqueta.

Busque la fila que contiene la etiqueta que se va a eliminar y haga clic en **Delete** en la columna **Operation**. En el cuadro de diálogo **Delete Tag** que se muestra, haga clic en **Yes**.

4 Monitoreo

4.1 Métricas admitidas

Descripción

Esta sección describe las métricas reportadas por NAT Gateway a Cloud Eye, así como sus espacios de nombres, métricas de supervisión y dimensiones. Puede usar la consola de gestión o las API proporcionadas por Cloud Eye para consultar las métricas generadas para NAT Gateway.

Espacio de nombres

SYS.NAT

Métricas

Tabla 4-1 métricas de Gateway NAT público

ID de métrica	Nombre	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (datos brutos)
snat_connection	SNAT Connections	Número de conexiones SNAT del gateway de NAT Unidad: Vez	≥ 0	Gateway NAT público	1 minuto
inbound_bandwidth	Inbound Bandwidth	Ancho de banda entrante de los servidores que utilizan la función de SNAT Unidad: bit/s	≥ 0 bits/s	Gateway NAT público	1 minuto

ID de métrica	Nombre	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (datos brutos)
outbound_bandwidth	Outbound Bandwidth	Ancho de banda saliente de los servidores que utilizan la función de SNAT Unidad: bit/s	≥ 0 bits/s	Gateway NAT público	1 minuto
inbound_pps	Inbound PPS	PPS entrantes de los servidores que utilizan la función SNAT Unidad: Vez	≥ 0	Gateway NAT público	1 minuto
outbound_pps	Outbound PPS	PPS saliente de los servidores que utilizan la función SNAT Unidad: Vez	≥ 0	Gateway NAT público	1 minuto
inbound_traffic	Inbound Traffic	Tráfico entrante de servidores que utilizan la función SNAT Unidad: byte	≥ 0 bytes	Gateway NAT público	1 minuto
outbound_traffic	Outbound Traffic	Tráfico saliente de servidores que utilizan la función SNAT Unidad: byte	≥ 0 bytes	Gateway NAT público	1 minuto
snat_connection_ratio	SNAT Connection Usage	Uso de la conexión SNAT de la gateway NAT El número máximo de conexiones es el número de conexiones permitidas por un tipo de gateway NAT. Para obtener más información, consulte Tipos de gateway de NAT . Unidad: Porcentaje	≥ 0	Gateway NAT público	1 minuto

ID de métrica	Nombre	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (datos brutos)
inbound_bandwidth_ratio	Inbound Bandwidth Usage	Uso de ancho de banda entrante de servidores que utilizan la función SNAT. El ancho de banda máximo soportado por un gateway de NAT público es de 20 Gbit/s. Unidad: Porcentaje	≥ 0	Gateway NAT público	1 minuto
outbound_bandwidth_ratio	Outbound Bandwidth Usage	Uso de ancho de banda saliente de los servidores que utilizan la función SNAT El ancho de banda máximo soportado por un gateway de NAT público es de 20 Gbit/s. Uso de ancho de banda saliente = Ancho de banda usado/Ancho de banda máximo del gateway de NAT público x 100%. Unidad: Porcentaje NOTA Esta métrica se utiliza para supervisar el rendimiento de los gateway de NAT públicos en lugar del ancho de banda de EIP.	≥ 0	Gateway NAT público	1 minuto

Tabla 4-2 Métricas de gateway de NAT privado

ID de métrica	Nombre	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (datos brutos)
snat_connection	SNAT Connections	Número de conexiones SNAT del gateway de NAT Unidad: Vez	≥ 0	Gateway de NAT privado	1 minuto
inbound_bandwidth	Inbound Bandwidth	Ancho de banda entrante de los servidores que utilizan la función de SNAT Unidad: bit/s	≥ 0 bit/s	Gateway de NAT privado	1 minuto
outbound_bandwidth	Outbound Bandwidth	Ancho de banda saliente de los servidores que utilizan la función de SNAT Unidad: bit/s	≥ 0 bit/s	Gateway de NAT privado	1 minuto
inbound_pps	Inbound PPS	PPS entrantes de los servidores que utilizan la función SNAT Unidad: Vez	≥ 0	Gateway de NAT privado	1 minuto
outbound_pps	Outbound PPS	PPS saliente de los servidores que utilizan la función SNAT Unidad: Vez	≥ 0	Gateway de NAT privado	1 minuto

ID de métrica	Nombre	Descripción	Rango de valores	Objeto monitoreado	Período de monitoreo (datos brutos)
inbound_traffic	Inbound Traffic	Tráfico entrante de servidores que utilizan la función SNAT Unidad: byte	≥ 0 bytes	Gateway de NAT privado	1 minuto
outbound_traffic	Outbound Traffic	Tráfico saliente de servidores que utilizan la función SNAT Unidad: byte	≥ 0 bytes	Gateway de NAT privado	1 minuto

Dimensiones


Clave	Valor
nat_gateway_id	Gateway NAT público ID
vpc_nat_gateway_id	Private NAT gateway ID

4.2 Creación de reglas de alarma

Escenarios

Puede establecer reglas de alarma de gateway de NAT para personalizar los objetos supervisados y las políticas de notificación. A continuación, puede aprender el estado de ejecución del gateway NAT de manera oportuna.

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 **Management & Deployment**, seleccione Cloud Eye.


4. En el panel de navegación izquierdo, elija **Alarm Management > Alarm Rules**.
5. En la página **Alarm Rules**, haga clic en **Create Alarm Rule** y establezca los parámetros necesarios para crear una regla de alarma o modificar una regla de alarma existente.
6. En la página **Create Alarm Rule**, siga las indicaciones para configurar los parámetros.
 - a. Establezca el nombre y la descripción de la regla de alarma.

Tabla 4-3 Configuración del nombre y descripción de la regla de alarma

Parámetro	Descripción
Name	Especifica el nombre de la regla de alarma. El sistema genera un nombre aleatorio, que puede modificar. Ejemplo de valor: alarm-b6al
Description	(Opcional) Proporciona información adicional acerca de la regla de alarma.

- b. Seleccione un objeto que se va a supervisar y establezca los parámetros de regla de alarma.

Tabla 4-4 Parámetros

Parámetro	Descripción	Valor de ejemplo
Resource Type	Especifica el tipo del recurso para el que se crea la regla de alarma.	NAT Gateway
Dimension	Especifica la dimensión métrica del tipo de recurso seleccionado.	Public NAT Gateway
Monitoring Scope	Especifica el ámbito de supervisión al que se aplica la regla de alarma. Puede seleccionar Resource groups o Specific resources . NOTA <ul style="list-style-type: none"> ● Si se selecciona Resource groups y cualquier recurso del grupo cumple la política de alarma, se activa una alarma. ● Si selecciona Specific resources, seleccione uno o más recursos y haga clic en  para agregarlos al cuadro de la derecha. 	Specific resources
Method	Hay dos opciones: Use template o Create manually .	Create manually
Template	Especifica la plantilla que se va a utilizar. Puede seleccionar una plantilla de alarma predeterminada o personalizar una plantilla.	N/A

Parámetro	Descripción	Valor de ejemplo
Alarm Policy	Especifica la política para activar una alarma. Si estableces Resource Type en Website Monitoring , Log Monitoring , Custom Monitoring o un servicio en la nube específico, si se activa una alarma depende de si los datos de métrica en periodos consecutivos alcanzan el umbral. Por ejemplo, Cloud Eye activa una alarma si los datos sin procesar de las conexiones SNAT del objeto monitorizado son 8000 o más durante tres periodos consecutivos de 1 minuto.	N/A
Alarm Severity	Especifica la gravedad de la alarma, que puede ser Critical , Major , Minor , o Informational .	Mayor

- c. Configure la notificación de alarma.

Tabla 4-5 Parámetros de notificación de alarma

Parámetro	Descripción
Alarm Notification	Especifica si se debe notificar a los usuarios cuando se activan las alarmas. Las notificaciones se pueden enviar por correo electrónico, mensaje de texto o mensaje HTTP/HTTPS.
Notification Object	Especifica el objeto que recibe las notificaciones de alarma. Puede seleccionar el contacto de la cuenta o un tema. <ul style="list-style-type: none"> ● Account contact es el número de teléfono móvil y la dirección de correo electrónico de la cuenta registrada. ● Un tema se utiliza para publicar mensajes y suscribirse a notificaciones. Si el tema requerido no está disponible, cree uno primero y agréguele suscripciones. Para obtener más información, consulte la Guía del usuario de Cloud Eye.
Validity Period	Cloud Eye envía notificaciones solo dentro del período de validez especificado en la regla de alarma. Si Validity Period se establece en 08:00-20:00 , Cloud Eye envía notificaciones solo entre las 08:00-20:00.
Trigger Condition	Especifica la condición que activa la notificación de alarma. Puede seleccionar Generated alarm (cuando se genera una alarma), Cleared alarm (cuando se borra una alarma) o ambos.

7. Después de establecer los parámetros, haga clic en **Create**.
 Una vez establecida la regla de alarma, el sistema le notifica automáticamente cuando se activa una alarma.

 **NOTA**

Para obtener más información acerca de cómo configurar las reglas de alarma, consulte [Creación de reglas de alarma](#).

4.3 Consulta de métricas

Prerrequisitos

- El gateway de NAT se está ejecutando correctamente y se han creado las reglas SNAT.
- Puede tomar un período de tiempo para obtener y transferir los datos de monitoreo. Por lo tanto, espere un rato y luego compruebe los datos.

Escenarios

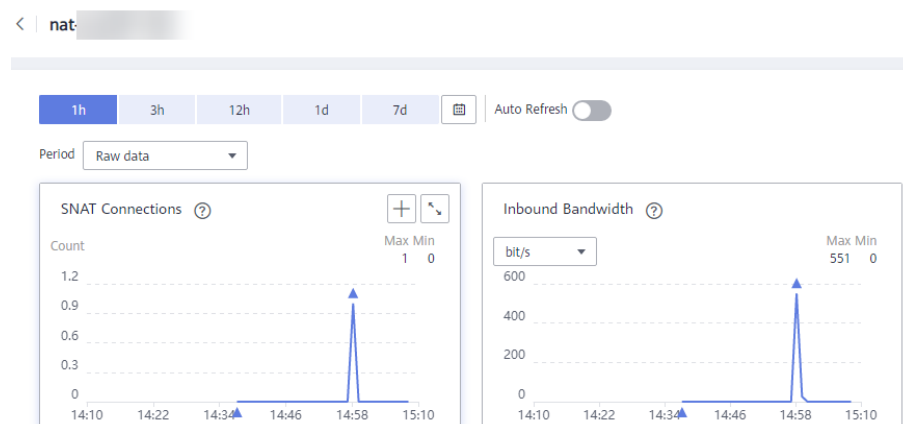
Esta sección describe cómo ver las métricas de NAT Gateway.

Procedimiento

1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda, seleccione la región de destino.
3. En **Management & Deployment**, seleccione Cloud Eye.
4. En el panel de navegación de la izquierda, elija **Cloud Service Monitoring > NAT Gateway**.
5. Busque la fila que contiene la métrica de destino y haga clic en **View Metric** en la columna **Operation** para comprobar la información detallada.

Puede ver los datos de la última, antepenúltima, 12 o 24 horas, o los últimos 7 días.

Figura 4-1 Consulta de métricas




4.4 Consulta de métricas de recursos mediante un gateway de NAT

Escenarios


Puede ver los detalles de las métricas de los recursos utilizando un gateway NAT específico. Los recursos pueden ser ECS o BMS.

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 la esquina superior izquierda. En **Networking** seleccione **NAT Gateway**.

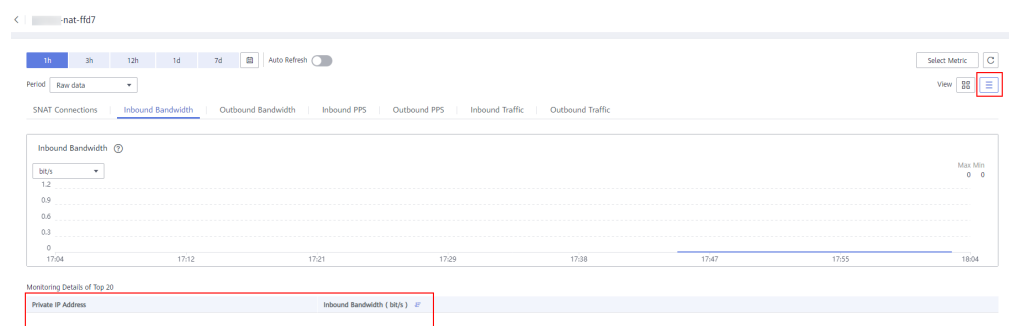
Se muestra la consola de gateway NAT.

4. Haga clic en el nombre de la gateway NAT cuyas métricas desea ver.
5. En la página mostrada, elija la ficha **Monitoring** y haga clic en **View Details**.
En la consola de Cloud Eye, vea las métricas de NAT Gateway.
6. Configure un intervalo de tiempo para que las métricas se vean.

7. Haga clic en  en la esquina superior derecha de la página para cambiar el modo de visualización.
8. Seleccione una métrica que desea ver y haga clic en un punto de tiempo específico en el gráfico que se muestra.

En la parte inferior de la página, puede ver los detalles de la métrica de los recursos en el punto de tiempo.

Figura 4-2 Consulta de métricas



5 Auditoría

5.1 Operaciones de clave registradas por CTS

Puede usar CTS para registrar operaciones en NAT Gateway para consulta, auditoría y seguimiento.

Tabla 5-1 enumera las operaciones públicas del gateway de NAT que pueden ser registradas por CTS.

Tabla 5-1 Operaciones pública de gateway de NAT

Operación	Tipo de recurso	Trazado
Creación de un gateway NAT público	natgateway	createNatGateway
Modificación de un gateway NAT público	natgateway	updateNatGateway
Eliminación de un gateway NAT público	natgateway	deleteNatGateway
Creación de una regla de DNAT	dnatrule	createDnatRule
Modificación de una regla de la DNAT	dnatrule	updateDnatRule
Eliminación de una regla de DNAT	dnatrule	deleteDnatRule
Creación de una regla SNAT	snatrule	createSnatRule
Modificación de una regla SNAT	snatrule	updateSnatRule
Eliminación de una regla SNAT	snatrule	deleteSnatRule

5.2 Consulta de trazas

Escenarios

CTS registra las operaciones realizadas en NAT Gateway y le permite ver los registros de operaciones de los últimos siete días en la consola CTS. En este tema se describe cómo consultar estos registros.

Procedimiento



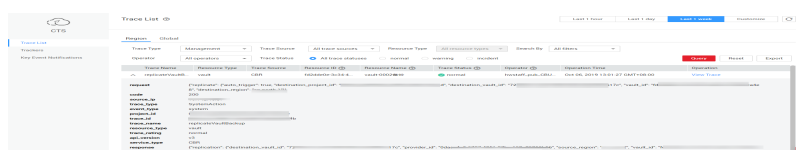
1. Inicie sesión en la consola de gestión.
2. En la esquina superior izquierda de la página, haga clic en  y seleccione la región y el proyecto deseados.
3. En **Management & Deployment**, haga clic en **Cloud Trace Service**.
4. En el panel de navegación de la izquierda, elija **Trace List**.
5. Especifique los filtros utilizados para consultar seguimientos. Los siguientes filtros están disponibles:
 - **Trace Type, Trace Source, Resource Type, y Search By**
 Seleccione un filtro de la lista desplegable.
 Si selecciona **Trace name** para **Search By**, seleccione un nombre de seguimiento específico.
 Si selecciona **Resource ID** para **Search By**, seleccione o introduzca un Id. de recurso específico.
 Si selecciona **Resource name** para **Search By**, seleccione o introduzca un nombre de recurso específico.
 - **Operator**: Seleccione un operador específico (en el nivel de usuario en lugar de en el nivel de tenant).
 - **Trace Status**: las opciones disponibles incluyen **All trace statuses, normal, warning, y incident**. Solo se puede habilitar una de ellas.
 - Intervalo de tiempo: Puede consultar las trazas generadas en cualquier intervalo de tiempo de los últimos siete días.
6. Haga clic en  a la izquierda de la traza requerida para ampliar sus detalles.

Figura 5-1 Ampliación de los detalles de seguimiento



7. Haga clic en **View Trace** en la columna **Operation** para ver los detalles del seguimiento.

Figura 5-2 Consulta de traza

```
"context": {
  "code": "204",
  "source_ip": "10.45.152.59",
  "trace_type": "ApiCall",
  "event_type": "system",
  "project_id": "0503dda89700fed2f78c00909158a4d",
  "trace_id": "116a2aff-deb8-11e9-95f5-d5c0b02a9b97",
  "trace_name": "deleteMember",
  "resource_type": "member",
  "trace_rating": "normal",
  "api_version": "v2.0",
  "service_type": "ELB",
  "response": "{\"member\": {\"project_id\": \"0503dda89700fed2f78c00909158a4d\", \"name\": \"9646e73b-338c-4d27-a17c-219be532812c\"}},",
  "resource_id": "9646e73b-338c-4d27-a17c-219be532812c",
  "tracker_name": "system",
  "time": "1569321775225",
  "resource_name": "9646e73b-338c-4d27-a17c-219be532812c",
  "record_time": "1569321775903",
  "user": {
    "domain": {
      "name": "huaweicloud.com",
      "id": "0503dda87800fed0f75c0096d70a960"
    }
  }
},
```

Para obtener detalles acerca de los campos clave en el seguimiento, consulte la sección "Estructura de traza" en la [Guía del usuario de Cloud Trace Service](#).