NAT Gateway

User Guide

Issue 01
Date 2024-08-12

Contents

1 Public NAT Gateways

1.1 Public NAT Gateway Overview

A public NAT gateway enables cloud and on-premises servers in a private subnet to access the Internet or provide services accessible from the Internet. Cloud servers are ECSs and BMSs in a VPC. On-premises servers are servers in on-premises data centers that connect to a VPC through Direct Connect or VPN. A public NAT gateway supports up to 20 Gbit/s of bandwidth.

The process of using a public NAT gateway is as follows.

Figure 1-1 Process of using a public NAT gateway
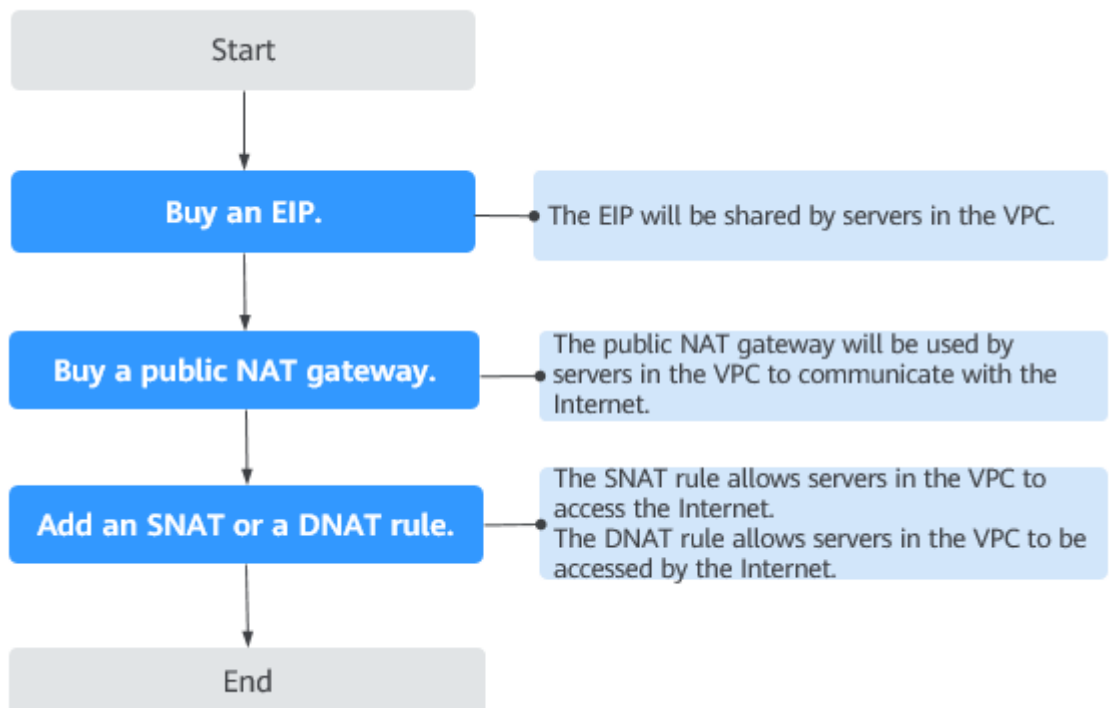
1.2 Managing Public NAT Gateways

1.2.1 Buying a Public NAT Gateway

Scenarios

Buy a public NAT gateway to enable your servers to access the Internet or provide services accessible from the Internet.

Constraints and Limitations

- Rules on one public NAT gateway can use the same EIP, but rules on different NAT gateways must use different EIPs.
- Each VPC can be associated with multiple public NAT gateways.
- The public NAT gateway does not translate IP addresses for Enterprise Edition VPN.
- If both an EIP and a public NAT gateway are configured for a server, data will be forwarded through the EIP.
- Some carriers will block the following ports for security reasons. It is recommended that you do not use the following ports.

Protocol	Port
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

Prerequisites

- The VPC and subnet where your public NAT gateway will be deployed are available.
- To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you buy a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you buy the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. On the displayed page, click **Buy Public NAT Gateway**.

5. Configure required parameters. For details, see **Table 1-1**.

Table 1-1 Descriptions of public NAT gateway parameters

Parameter	Description
Billing Mode	Public NAT gateways are billed on a pay-per-use basis.
Region	The region where the public NAT gateway is located
Name	The name of the public NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.
VPC	The VPC that the public NAT gateway belongs to The selected VPC cannot be changed after you buy the public NAT gateway. **NOTE** To allow traffic to pass through the public NAT gateway, a route to the public NAT gateway in the VPC is required. When you buy a public NAT gateway, a default route 0.0.0.0/0 to the public NAT gateway is automatically added to the default route table of the VPC. If the default route 0.0.0.0/0 already exists in the default route table of the VPC before you buy the public NAT gateway, the default route that points to the public NAT gateway will fail to be added automatically. In this case, perform the following operations after the public NAT gateway is successfully created: Manually add a different route that points to the gateway or create a default route 0.0.0.0/0 pointing to the gateway in the new routing table.
Subnet	The subnet that the public NAT gateway belongs to The subnet must have at least one available IP address. The selected subnet cannot be changed after you buy the public NAT gateway. The NAT gateway will be deployed in the selected subnet. The NAT gateway works for the entire VPC where it is deployed. To enable communications over the Internet, add SNAT or DNAT rules.
Specifications	The specifications of the public NAT gateway The value can be **Extra-large**, **Large**, **Medium**, or **Small**. To view more details about specifications, click **Learn more** on the page.

Parameter	Description
Enterprise Project	The enterprise project that the public NAT gateway belongs to If an enterprise project has been configured, select the enterprise project. If you have not configured any enterprise project, select the **default** enterprise project.
Description	Supplementary information about the public NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.
Tag	Specifies the identifier of the public NAT gateway. A tag is a key-value pair. You can add up to 10 tags to each NAT gateway. If you have configured tag policies for public NAT gateways, you need to add tags to your public NAT gateways based on the tag policies. If you add a tag that does not comply with the tag policies, public NAT gateways may fail to be created. Contact your administrator to learn more about tag policies. The tag key and value must meet the requirements listed in **Table 1-2**.

Table 1-2 Tag requirements

Parameter	Requirement
Key	● Cannot be left blank. ● Must be unique for each NAT gateway. ● Can contain a maximum of 36 characters. ● Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/), and the first and last characters cannot be spaces.
Value	● Can contain a maximum of 43 characters. ● Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/), and the first and last characters cannot be spaces.

After you configure the parameters, the public NAT gateway price will be displayed. To view more pricing details, click **Pricing details** on the page.

6. Click **Next**. On the page displayed, confirm the public NAT gateway specifications.

7. Click **Submit**.

It takes 1 to 6 minutes to create a public NAT gateway.

8. In the list, view the status of the public NAT gateway.

Adding a Default Route Pointing to the Public NAT Gateway

1. Log in to the management console.

2. Click [icon] in the upper left corner and select the desired region and project.

3. Under **Networking**, select **Virtual Private Cloud**.

4. In the navigation pane on the left, choose **Route Tables**.

5. On the **Route Tables** page, click **Create Route Table** in the upper right corner.
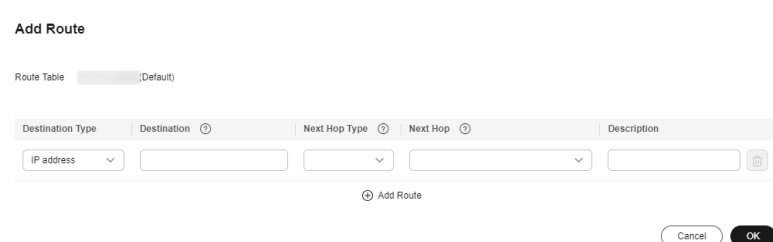
   VPC: Select the VPC to which the public NAT gateway belongs.

   > **NOTE**
   >
   > If the custom route table quota is insufficient, **create a service ticket** to increase the route table quota.

6. After the custom route table is created, click its name.

   The **Summary** page is displayed.

7. Click **Add Route** and configure parameters as follows:

   Destination: Set it to **0.0.0.0/0**.

   Next Hop Type: Select **NAT gateway**.

   Next Hop: Select the created NAT gateway.

   Figure 1-2 Add Route

8. Click **OK**.

   > **NOTE**
   >
   > After the public NAT gateway is created, check whether a default route (0.0.0.0/0) that points to the public NAT gateway exists in the default route table of the VPC where the public NAT gateway is. If no, add a route pointing to the public NAT gateway to the default route table, alternatively, create a custom route table and add the default route 0.0.0.0/0 pointing to the public NAT gateway to the table. The following describes how to add a route to a custom route table.

1.2.2 Viewing a Public NAT Gateway

Scenarios

View information about a public NAT gateway.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. View information about the public NAT gateway.

1.2.3 Modifying a Public NAT Gateway

Scenarios

Modify the name, specifications, or description of a public NAT gateway.

Using a public NAT gateway of more robust specifications does not affect services, but if you switch to a public NAT gateway of less robust specifications, ensure that its capacity can still be enough to meet your service requirements.

Prerequisites

A public NAT gateway is available.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Locate the row that contains the public NAT gateway you want to modify and click **Modify** in the **Operation** column.

5. Modify the name, specifications, or description of the public NAT gateway.

Figure 1-3 Modify NAT Gateway

6. Click **OK**.

1.2.4 Deleting or Unsubscribing from a Public NAT Gateway

Scenarios

Delete or unsubscribe from public NAT gateways that are no longer required to release resources and reduce costs.

📖 **NOTE**

● To unsubscribe from a pay-per-use public NAT gateway, you need to **delete the NAT gateway**.

Prerequisites

● All SNAT and DNAT rules created on the public NAT gateway have been deleted. For details about how to delete SNAT and DNAT rules, see **Deleting an SNAT Rule** and **Deleting a DNAT Rule**.

Procedure

1. Log in to the management console.
2. Click ⊙ in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

    The **Public NAT Gateway** page is displayed.
4. On the displayed page, locate the public NAT gateway that you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, enter **DELETE**.
6. Click **OK**.

1.3 Managing SNAT Rules

1.3.1 Adding an SNAT Rule

Scenarios

After a public NAT gateway is created, add an SNAT rule, so that servers in a VPC subnet or servers that are connected to a VPC through Direct Connect or Cloud Connect can access the Internet by sharing an EIP.

One SNAT rule takes effect for only one subnet. If there are multiple subnets in a VPC, create multiple SNAT rules to allow servers in them to share EIPs.

Constraints and Limitations

- Only one SNAT rule can be added for each VPC subnet.
- When you add an SNAT rule in the VPC scenario, the custom CIDR block must be a subset of the NAT gateway's VPC subnets.
- If an SNAT rule is used in the Direct Connect scenario, the custom CIDR block must be a CIDR block of a Direct Connect connection and cannot overlap with the NAT gateway's VPC subnets.
- There is no limit on the number of SNAT rules that can be added on a public NAT gateway.

Prerequisites

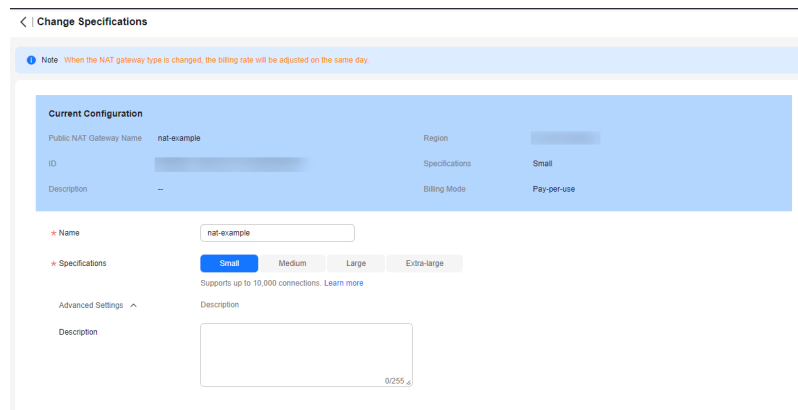A public NAT gateway is available.

Procedure

1. Log in to the management console.
2. Click ⊙ in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.
   The **Public NAT Gateway** page is displayed.
4. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
5. On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 1-4 Add SNAT Rule
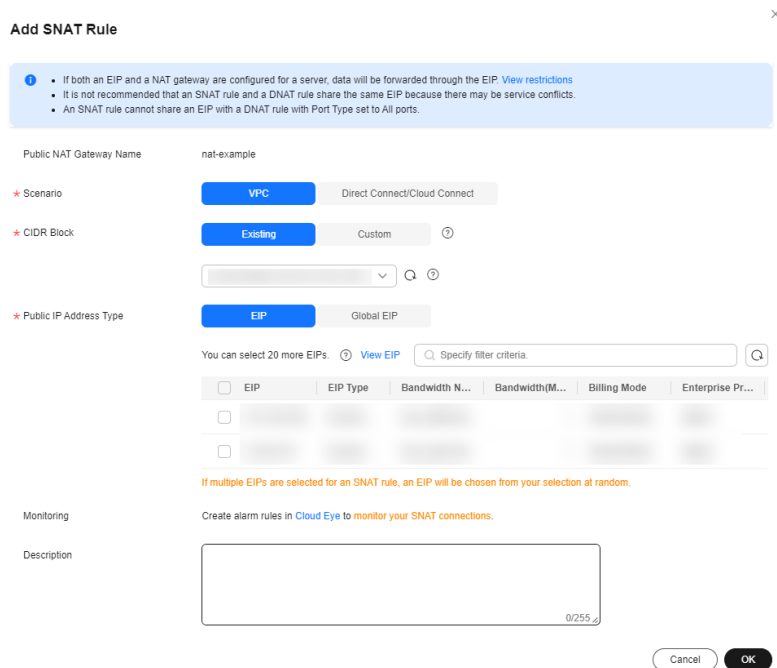
6. Configure required parameters. For details, see **Table 1-3**.

Table 1-3 Descriptions of SNAT rule parameters

Parameter	Description
Scenario	The scenarios where the SNAT rule is used Select **VPC** if your servers in a VPC need to access the Internet. Select **Direct Connect/Cloud Connect** if servers in your on-premises data center or in another VPC need to access the Internet.
Subnet	● **Existing**: Select an existing subnet. ● **Custom**: Customize a CIDR block or enter a server IP address. NOTE When you select **Custom**, you can enter 0.0.0.0/0. Only a 32-bit server IP address is supported.
Public IP Address Type	The EIP used for accessing the Internet You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with **Port Type** set to **Specific port**, or has been bound to an SNAT rule of the current public NAT gateway. You can select up to 20 EIPs for an SNAT rule. If you have selected multiple EIPs for an SNAT rule, one EIP will be chosen randomly.

Parameter	Description
Monitoring	You can create alarm rules on the Cloud Eye console to monitor your SNAT connections and keep informed of any changes in a timely manner.
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

7. Click **OK**.

☰ NOTE

- You can add multiple SNAT rules for a public NAT gateway to suite your service requirements.
- Each VPC can be associated with multiple public NAT gateways.
- Only one SNAT rule can be added for each VPC subnet.

1.3.2 Viewing an SNAT Rule

Scenarios

View details about an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. In the SNAT rule list, view details about the SNAT rule.

1.3.3 Modifying an SNAT Rule

Scenarios

Modify an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⦾ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.

6. Click **Modify** in the **Operation** column.

7. In the displayed dialog box, modify parameters as needed.

8. Click **OK**.

1.3.4 Deleting an SNAT Rule

Scenarios

Delete an SNAT rule that you no longer need.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⦾ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.

6. Enter **DELETE** in the displayed dialog box and click **OK**.

1.4 Managing DNAT Rules

1.4.1 Adding a DNAT Rule

Scenarios

After a public NAT gateway is created, add DNAT rules to allow servers in your VPC to provide services accessible from the Internet.

Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP. If multiple servers need to provide services accessible from the Internet, create multiple DNAT rules.

Restrictions and Limitations

- Only one DNAT rule can be configured for each port on a server. One port can be mapped to only one EIP.
- A maximum of 200 DNAT rules can be added on a public NAT gateway.

Prerequisites

A public NAT gateway is available.

Procedure
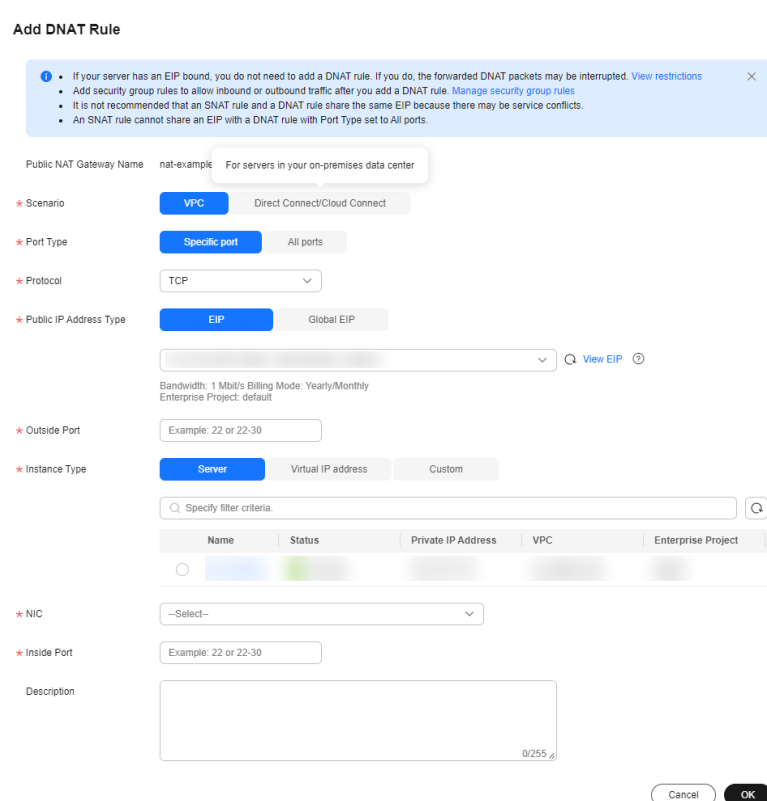
1. Log in to the management console.
2. Click ⚲ in the upper left corner and select the desired region and project.
3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.
4. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
5. On the public NAT gateway details page, click the **DNAT Rules** tab.
6. Click **Add DNAT Rule**.

   Figure 1-5 Add DNAT Rule

7. Configure required parameters. For details, see **Table 1-4**.

Table 1-4 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	Select **VPC** if your servers in a VPC will use the DNAT rule to share the same EIP to provide services accessible from the Internet. **Direct Connect/Cloud Connect**: Select this scenario if your on-premises servers or servers in another VPC will use the DNAT rule to provide services accessible from the Internet.
Port Type	The port type ● **All ports**: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server. ● **Specific port**: Only requests received from a specified port over a specified protocol will be forwarded to the specified port on the server.
Protocol	The protocol can be TCP or UDP. This parameter is available if you select **Specific port** for **Port Type**. If you select **All ports**, the value of this parameter is **All** by default.
Public IP Address Type	The EIP that will be used by the server to provide services accessible from the Internet You can select an EIP that either has not been bound, has been bound to a DNAT rule of the current public NAT gateway with **Port Type** set to **Specific port**, or has been bound to an SNAT rule of the current public NAT gateway.
Outside Port	The port of the EIP used by the NAT gateway for external communication This parameter is only available if you select **Specific port** for **Port Type**. Range: 1 to 65535 You can enter a specific port number or a port range, for example, 80 or 80-100.
Instance Type	The type of the instance that will be providing services accessible from the Internet. Possible values are: ● **Server** ● **Virtual IP address** ● **Custom**
NIC	The NIC of the server. This parameter is available if you set **Instance Type** to **Server**.

Parameter	Description
Private IP Address	- In a VPC scenario, set this parameter to the private IP address of a server in the NAT gateway's VPC. The server will provide services accessible from the Internet through DNAT. - In a Direct Connect/Cloud Connect scenario, set this parameter to IP address of the server in your on-premises data center or your private IP address. This IP address is used by on-premises servers that are connected to a VPC through Direct Connect or servers in another VPC to provide services accessible from the Internet through DNAT. - Configure the port of **Private IP Address** if you select **Specific port** for **Port Type**.
Inside Port	The port of the server over which the originating requests will be forwarded This parameter is only available if you select **Specific port** for **Port Type**. Range: 1 to 65535 You can enter a specific port number or a port range, for example, 80 or 80-100.
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

8. Click **OK**.

   Once the rule is created, its status changes to **Running**.

> **NOTICE**
>
> After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

1.4.2 Viewing a DNAT Rule

Scenarios

View details about a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. On the public NAT gateway details page, click the **DNAT Rules** tab.

6. In the DNAT rule list, view details about the DNAT rule.

1.4.3 Modifying a DNAT Rule

Scenarios

Modify a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. On the public NAT gateway details page, click the **DNAT Rules** tab.

6. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.

7. In the displayed dialog box, modify parameters as needed.

8. Click **OK**.

1.4.4 Deleting a DNAT Rule

Scenarios

Delete a DNAT rule that you no longer need.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. On the public NAT gateway details page, click the **DNAT Rules** tab.

6. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.

7. Enter **DELETE** in the displayed dialog box and click **OK**.

1.4.5 Deleting DNAT Rules in Batches

Scenarios

Delete DNAT rules that you no longer need.

Prerequisites

DNAT rules have been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. Click the name of the public NAT gateway.

5. On the public NAT gateway details page, click the **DNAT Rules** tab.

6. In the DNAT rule list, select DNAT rules that you no longer need and click **Delete DNAT Rule**.

7. In the displayed dialog box, click **Yes**.

1.4.6 Importing DNAT Rules by Using a Template and Exporting DNAT Rules

Scenarios

When adding DNAT rules in different environments or migrating DNAT rules between NAT gateways, you can import and export DNAT rules to simplify and accelerate the DNAT rule configuration.

Prerequisites

A public NAT gateway is available.

Importing DNAT Rules

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. On the displayed page, click the name of the public NAT gateway to which you want to import DNAT rules.

5. On the public NAT gateway details page, click the **DNAT Rules** tab.

6. On the displayed page, click **Import**. In the displayed **Import Rule** dialog box, click **Download Template**.

7. Fill in DNAT rule parameters based on the table heading in the template. For details, see **Table 1-5**.

Table 1-5 Descriptions of DNAT rule parameters

Parameter	Description
Scenario	The following two scenarios are available: ● **VPC**: The servers in a VPC will share an EIP to provide services accessible from the Internet through the DNAT rule. ● **Direct Connect/Cloud Connect**: Select this scenario if your on-premises servers or servers in another VPC will use the DNAT rule to provide services accessible from the Internet.
Protocol	The value can be **TCP**, **UDP**, or **All**.
EIP	The EIP that will be used by the server to provide publicly accessible services Only EIPs that have not been bound or that have been bound to a DNAT rule in the current VPC are available for selection.
Outside Port	The EIP port This parameter is only available if **Specific port** is selected for **Port Type**. You can enter a specific port number or a port range, for example, 80 or 80-100.

Parameter	Description
Private IP Address	• In a VPC scenario, set this parameter to the private IP address of a server in the NAT gateway's VPC. The server will provide services accessible from the Internet through DNAT. • In a Direct Connect/Cloud Connect scenario, set this parameter to IP address of the server in your on-premises data center or your private IP address. This IP address is used by on-premises servers that are connected to a VPC through Direct Connect or servers in another VPC to provide services accessible from the Internet through DNAT. • Configure the private IP address port if **Protocol** is set to **TCP** or **UDP**.
Inside Port	• In a VPC scenario, set this parameter to the port of the server in a VPC. • In a Direct Connect/Cloud Connect scenario, set this parameter to the port of the server in the on-premises data center or the user's private port. • This parameter is only available if **Specific port** is selected for **Port Type**. The number of inside and outside ports must match.
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Open angle brackets (<), close angle brackets (>), and angle brackets (<>) are not allowed.

8. After filling in the template, click **Select File**, select the local template, and click **Import**.

    Figure 1-6 Import Rule
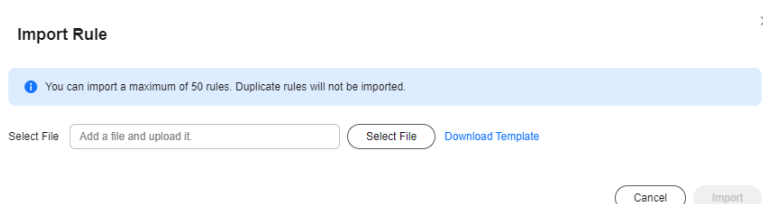
9. View the imported DNAT rules.

    If their **Status** is **Running**, the DNAT rules have been added.

Exporting DNAT Rules

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The **Public NAT Gateway** page is displayed.

4. On the displayed page, click the name of the public NAT gateway from which you want to export DNAT rules.

5. On the public NAT gateway details page, click the **DNAT Rules** tab.

6. In the DNAT rule list, select the rules to be exported and click **Export** above the list.

2 Private NAT Gateways

2.1 Private NAT Gateway Overview

Private NAT Gateways

Private NAT gateways provide private address translation services for ECSs and BMSs in a VPC. You can configure SNAT and DNAT rules to translate the source and destination IP addresses into transit IP addresses, so that servers in the VPC can communicate with other VPCs or on-premises data centers.

Specifically:

- SNAT enables servers across AZs in a VPC to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers across AZs in a VPC to share a transit IP address to provide services accessible from on-premises data centers or other VPCs.

Transit Subnet

A transit subnet functions as a transit network. You can configure a transit IP address for the transit subnet so that servers in a local VPC can share the transit IP address to access on-premises data centers or other VPCs.

Transit VPC

The transit VPC is the VPC that the transit subnet is a part of.

Figure 2-1 Private NAT gateway
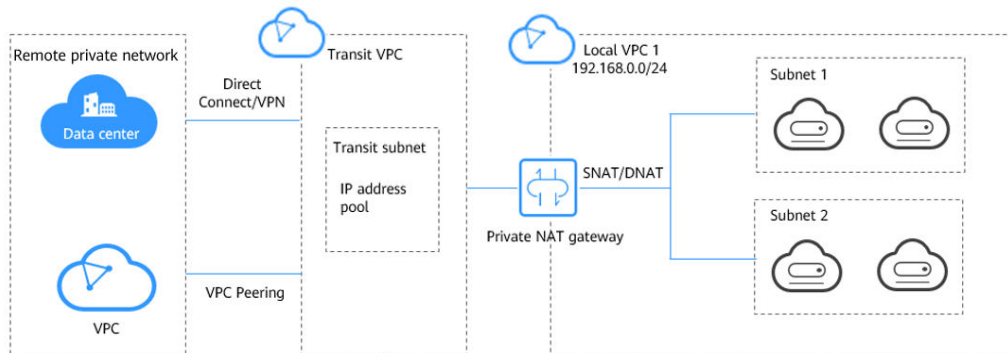
Differences Between Public and Private NAT Gateways

Public NAT gateways use SNAT rules to map private IP addresses to EIPs, so that servers in a VPC can share an EIP to access the Internet. DNAT rules enable the servers to share an EIP to provide services accessible from the Internet.

Private NAT gateways use SNAT rules to map private IP addresses to transit IP addresses, so that servers in a VPC can access on-premises data centers or other VPCs. DNAT rules enable the servers to share the transit IP address to provide services accessible from the private network.

Table 2-1 describes the differences between public and private NAT gateways.

Table 2-1 Differences between public and private NAT gateways

Item	Public NAT Gateway	Private NAT Gateway
Function	Connects a private network to the Internet	Connects private networks
SNAT	Enables access to the Internet	Enables access to on-premises data centers or other VPCs
DNAT	Allows servers to provide services accessible from the Internet	Allows servers to provide services accessible from on-premises data centers or other VPCs in private networks
Communications media	EIP	Transit IP address

Helpful Links

Using Private NAT Gateways to Enable Communications Between Cloud and On-premises Networks

2.2 Buying a Private NAT Gateway

2.2.1 Overview

This section describes how to deploy a private NAT gateway.

Figure 2-2 Process for deploying a private NAT gateway
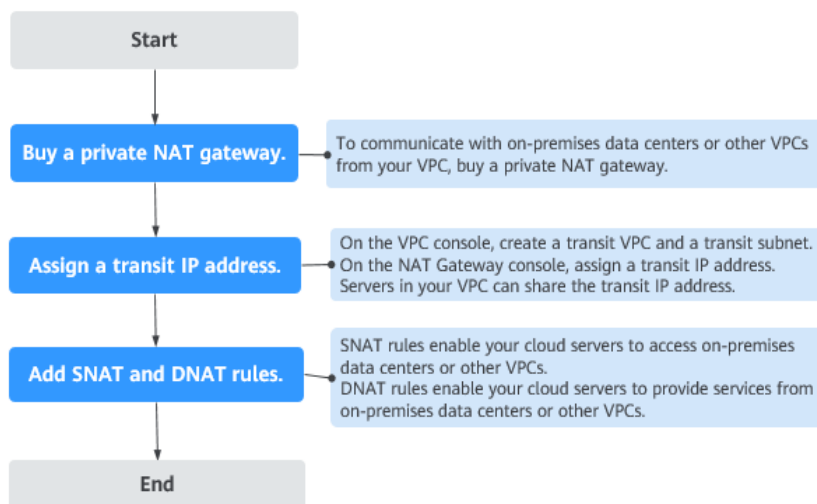
If you want to use a private NAT gateway to connect your VPC to on-premises data centers or other VPCs, refer to **Accessing On-premises Data Centers or Other VPCs**.

2.2.2 Buying a Private NAT Gateway

Scenarios

You can a private NAT gateway to enable servers in your VPC to access or provide services accessible from on-premises data centers and other VPCs.

Constraints and Limitations

- Manually add routes in a VPC to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
- SNAT and DNAT rules cannot share a transit IP address.
- The total number of DNAT and SNAT rules that can be added on a private NAT gateway varies with the private NAT gateway specifications.
  - Small: 20 or less
  - Medium: 50 or less
  - Large: 200 or less

– Extra-large: 500 or less

> ⚠️ **CAUTION**
>
> When you buy a private NAT gateway, you must specify its VPC, subnet, and specifications.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click **Buy Private NAT Gateway**.

6. Configure required parameters. For details, see **Table 2-2**.

Table 2-2 Descriptions of private NAT gateway parameters

Parameter	Description
Billing Mode	Private NAT gateways are billed on a pay-per-use basis.
Region	The region where the private NAT gateway is located
Name	The name of the private NAT gateway Enter up to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.
VPC	The VPC that the private NAT gateway belongs to The selected VPC cannot be changed after the private NAT gateway is purchased.
Subnet	The subnet that the private NAT gateway belongs to The subnet must have at least one available IP address. The selected subnet cannot be changed after the private NAT gateway is purchased.
Specifications	The specifications of the private NAT gateway The value can be **Extra-large**, **Large**, **Medium**, or **Small**. For details about specifications, see **NAT Gateway Specifications**.

Parameter	Description
Tag	The private NAT gateway tag, which consists of a key and value pair. You can add up to 10 tags to each private NAT gateway. If you have configured tag policies for private NAT gateways, add tags to your private NAT gateways based on the tag policies. If you add a tag that does not comply with the tag policies, private NAT gateways may fail to be created. Contact your administrator to learn more about tag policies. The tag key and value must meet the requirements listed in **Table 2-3**.
Description	Supplementary information about the private NAT gateway Enter up to 255 characters. Angle brackets (<>) are not allowed.

Table 2-3 Tag requirements

Parameter	Requirement
Key	● Cannot be left blank. ● Must be unique for each NAT gateway. ● Can contain a maximum of 36 characters. ● Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/), and the first and last characters cannot be spaces.
Value	● Can contain a maximum of 43 characters. ● Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/), and the first and last characters cannot be spaces.

7. Click **Buy Now**.

Helpful Links

Managing Private NAT Gateways

2.2.3 Assigning a Transit IP Address

Scenarios

After a private NAT gateway is created, assign a transit IP address, so that servers in your VPC can share the transit IP address to communicate with on-premises data centers or other VPCs.

Prerequisites

- There are transit VPCs and transit subnets available.
- A Direct Connect connection has been created with the VPC CIDR block set to **0.0.0.0/0**. For details, see **Create a Virtual Gateway**.

Procedure

1. Log in to the management console.

2. Click [ ] in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click **Transit IP Addresses**.

   Figure 2-3 Assign Transit IP Address

6. Configure required parameters. For details, see **Table 2-4**.

Table 2-4 Parameter descriptions of a transit IP address

Parameter	Description
Transit VPC	Specifies the VPC to which the transit IP address belongs.
Transit Subnets	A transit subnet is a transit network and is the subnet to which the transit IP address belongs. The subnet must have at least one available IP address.
Transit IP Address	The transit IP address can be assigned in either of the following ways: **Automatic**: The system automatically assigns a transit IP address. **Manual**: You need to manually assign a transit IP address.
IP Address	This parameter is only available when you set **Transit IP Address** to **Manual**.
Enterprise Project	Specifies the enterprise project to which the transit IP address belongs.

7. Click **OK**.

2.2.4 Adding an SNAT Rule

Scenarios

After the private NAT gateway is created, add an SNAT rule so that some or all servers in a VPC subnet can share a transit IP address to access on-premises data centers or other VPCs.

Constraints and Limitations

- Only one SNAT rule can be added for each VPC subnet.

Prerequisites

- A private NAT gateway is available.
- Transit IP addresses are available.
- A Direct Connect connection has been created with the VPC CIDR block set to **0.0.0.0/0**. For details, see **Create a Virtual Gateway**.

Procedure

1. Log in to the management console.

2. Click   in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add an SNAT rule.

6. On the **SNAT Rules** tab, click **Add SNAT Rule**.

7. Configure required parameters. For details, see **Table 2-5**.

Table 2-5 Parameter descriptions of an SNAT rule

Parameter	Description
Subnet	The subnet type of the SNAT rule. Select **Existing** or **Custom**. Select a subnet where IP address translation is required in the service VPC.
Monitoring	You can create alarm rules to watch the number of SNAT connections.
Transit IP Address	Select the created transit IP address.
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

8. Click **OK**.

📖 **NOTE**

You can add multiple SNAT rules for a private NAT gateway to suite your service requirements.

Helpful Links

Managing SNAT Rules

2.2.5 Adding a DNAT Rule

Scenarios

After a private NAT gateway is created, you can add DNAT rules to allow servers in your VPC to provide services accessible from on-premises servers or other VPCs.

A DNAT rule needs to be configured for each port on a server that needs to be made accessible. If multiple ports on a server or multiple servers need to provide services accessible from on-premises servers or other VPCs, multiple DNAT rules need to be configured.

Constraints and Limitations

- A DNAT rule with **Port Type** set to **All ports** cannot share a transit IP address with a DNAT rule with **Port Type** set to **Specific port**.

Prerequisites

- A private NAT gateway is available.

- Transit IP addresses are available.

Procedure

1. Log in to the management console.

2. Click [location icon] in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add a DNAT rule.

6. On the private NAT gateway details page, click the **DNAT Rules** tab.

7. Click **Add DNAT Rule**.

NOTICE

After you add a DNAT rule, add rules to the security group associated with the servers to allow inbound or outbound traffic. Otherwise, the DNAT rule does not take effect.

---

8. Configure required parameters. For details, see **Table 2-6**.

Figure 2-4 Add DNAT Rule

Table 2-6 Descriptions of DNAT rule parameters

Parameter	Description
Local Network	
Port Type	The port type
	The type can be:
	● **Specific port**: The private NAT gateway only forwards requests to your servers from the outside port and to the inside port configured here, and only if they use the right protocol.
	● **All ports**: All requests received by the gateway through all ports over any protocol will be forwarded to the private IP address of your server.
Protocol	The protocol can be TCP or UDP
	If you select **All ports**, the value of this parameter is **All** by default.
	This parameter is only available if you select **Specific port** for **Port Type**.
Instance Type	The type of instance that will provide services accessible from on-premises data centers or other VPCs
	Possible types are:
	● **Server**
	● **Virtual IP address**
	● **Load balancer**
	● **Custom**
NIC	The NIC of the server
	This parameter is only available if you set **Instance Type** to **Server**.
IP Address	The IP address of the server that will provide services accessible from on-premises data centers or other VPCs. This parameter is only available if you set **Instance Type** to **Custom**.
Internal Port	The port of the instance
	Range: 1 to 65535
	This parameter is only available if you select **Specific port** for **Port Type**.
Transit Network	

Parameter	Description
Transit IP Address	The transit IP address used to access on-premises data centers or other VPCs
	You can select a transit IP address that is not bound to any resource, has been bound to a DNAT rule for the current private NAT gateway where **Port Type** is set to **Specific port**, or has been bound to a SNAT rule of the current private NAT gateway.
Transit IP Address Port	The port of the transit IP address Supported range: 1 to 65535
	This parameter is only available if you select **Specific port** for **Port Type**.
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

9. Click **OK**.

   Once the rule is created, its status changes to **Running**.

Helpful Links

Managing DNAT Rules

2.3 Managing Private NAT Gateways

2.3.1 Viewing a Private NAT Gateway

Scenarios

View information about a private NAT gateway.

Prerequisites

A private NAT gateway is available.

Procedure

1. Log in to the management console.

2. Click in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

6. On the displayed page, view information about the private NAT gateway.

2.3.2 Modifying a Private NAT Gateway

Scenarios

Modify the name, specifications, or description of a private NAT gateway.

Prerequisites

A private NAT gateway is available.

Procedure

1. Log in to the management console.

2. Click ⦿ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, locate the row that contains the private NAT gateway you want to modify and click **Modify** in the **Operation** column.

6. Modify the name, specifications, or description of the private NAT gateway.

7. Click **Next**.

8. Confirm the modification and click **Submit**.

2.3.3 Deleting a Private NAT Gateway

Scenarios

Delete private NAT gateways that are no longer required to release resources and reduce costs.

Prerequisites

All SNAT and DNAT rules created on the private NAT gateway have been deleted. For details about how to delete SNAT and DNAT rules, see **Deleting an SNAT Rule** and **Deleting a DNAT Rule**.

Procedure

1. Log in to the management console.

2. Click ⦿ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, locate the private NAT gateway that you want to delete and click **Delete** in the **Operation** column.

6. In the displayed dialog box, enter **DELETE**.

7. Click **OK**.

2.4 Managing SNAT Rules

2.4.1 Viewing an SNAT Rule

Scenarios

View details about an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⦿ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

    The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

6. In the SNAT rule list, view details about the SNAT rule.

2.4.2 Modifying an SNAT Rule

Scenarios

Modify an SNAT rule.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

6. On the **SNAT Rules** tab, locate the row that contains the SNAT rule you want to modify.

7. Click **Modify** in the **Operation** column.

8. In the displayed dialog box, modify parameters as needed.

9. Click **OK**.

2.4.3 Deleting an SNAT Rule

Scenarios

Delete SNAT rules that you no longer need.

Prerequisites

An SNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

6. In the SNAT rule list, locate the row that contains the SNAT rule you want to delete and click **Delete** in the **Operation** column.

7. In the displayed dialog box, click **Yes**.

2.5 Managing DNAT Rules

2.5.1 Viewing a DNAT Rule

Scenarios

View details about a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

6. On the private NAT gateway details page, click the **DNAT Rules** tab.

7. In the DNAT rule list, view details about the DNAT rule.

2.5.2 Modifying a DNAT Rule

Scenarios

Modify a DNAT rule.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

6. On the private NAT gateway details page, click the **DNAT Rules** tab.

7. In the DNAT rule list, locate the row that contains the DNAT rule you want to modify and click **Modify** in the **Operation** column.

8. In the displayed dialog box, modify parameters as needed.

9. Click **OK**.

2.5.3 Deleting a DNAT Rule

Scenarios

Delete a DNAT rule that you no longer need.

Prerequisites

A DNAT rule has been added.

Procedure

1. Log in to the management console.

2. Click in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

6. On the private NAT gateway details page, click the **DNAT Rules** tab.

7. In the DNAT rule list, locate the row that contains the DNAT rule you want to delete and click **Delete** in the **Operation** column.

8. In the displayed dialog box, click **Yes**.

2.6 Managing Transit IP Addresses

2.6.1 Assigning a Transit IP Address

Scenarios

Servers in a VPC all use the same transit IP address to access or provide services accessible from on-premises data centers or other VPCs.

Procedure

1. Log in to the management console.

2. Click in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. On the **Private NAT Gateways** page, click **Transit IP Addresses**.

Figure 2-5 Assign Transit IP Address

6. Configure required parameters. For details, see **Table 2-7**.

Table 2-7 Parameter descriptions of a transit IP address

Parameter	Description
Transit VPC	VPC to which the transit IP address is located
Transit Subnet	A transit subnet is a transit network and is the subnet to which the transit IP address belongs. The subnet must have at least one available IP address.
Transit IP Address	The transit IP address can be assigned in either of the following ways: **Automatic**: The system automatically assigns a transit IP address. **Manual**: You need to manually assign a transit IP address.
IP Address	This parameter is only available when you set **Transit IP Address** to **Manual**.
Enterprise Project	The enterprise project to which the transit IP address belongs.

7. Click **OK**.

2.6.2 Viewing a Transit IP Address

Scenarios

View details about transit IP addresses assigned to you.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. Click the **Transit IP Addresses** tab and then click the transit IP address.

6. On the page displayed, view details about the assigned transit IP addresses.

2.6.3 Releasing a Transit IP Address

Scenarios

Release a transit IP address that you no longer need.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. In the navigation pane on the left, choose **NAT Gateway** > **Private NAT Gateways**.

5. In the **Transit IP Addresses** area, locate the transit IP address you want to release, and click **Release** in the **Operation** column.

6. Click **Yes**.

   > 📖 **NOTE**
   >
   > If a transit IP address has been associated with an SNAT or DNAT rule, it cannot be released. To release such a transit IP address, delete all rules associated with it first.

2.7 Accessing On-Premises Data Centers or Other VPCs

Accessing On-Premises Data Centers

You can use Direct Connect or VPN to connect the transit VPC to your on-premises data centers.

For a higher quality connection, use Direct Connect. For details, see **Overview**.

For more cost-effective connectivity, use VPN. For details, see **Overview.**

Accessing Other VPCs

You can use VPC Peering to connect the transit VPC to other VPCs.

For details, see **VPC Peering Connection Overview**.

3 Permissions Management

3.1 Creating a User and Granting NAT Gateway Permissions

This section describes how to use **IAM** to implement fine-grained permissions control for your NAT Gateway resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing NAT Gateway resources.

- Grant only the permissions required for users to perform a specific task.

- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your NAT Gateway resources.

If your Huawei Cloud account does not require individual IAM users, skip this section.

This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

Learn about the permissions supported by NAT Gateway and choose policies or roles according to your requirements. For details, see **Permissions**. For the permissions of other services, see **System-defined Permissions**.

Process Flow

Figure 3-1 Process for granting NAT Gateway permissions
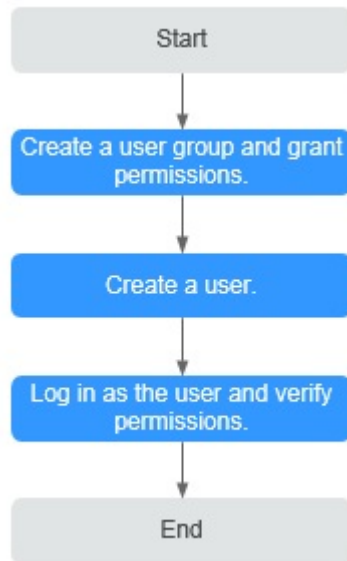
1. **Create a user group and assign permissions**.

   Create a user group on the IAM console, and attach the **ReadOnlyAccess** policy to the group.

2. **Create an IAM user and add it to a user group.**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console as the created user. Switch to the authorized region and verify the permissions.

   – Choose **Service List** > **NAT Gateway**. Then click **Buy NAT Gateway**. If a message appears indicating that you have insufficient permissions to perform the operation, the **ReadOnlyAccess** policy has already taken effect.

   – Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **ReadOnlyAccess** policy has already taken effect.

3.2 NAT Gateway Custom Policies

You can create custom policies to supplement system-defined policies of NAT Gateway. For the actions that can be added to custom policies, see **Permissions Policies and Supported Actions**.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. You do not need to have knowledge of the policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For operation details, see **Creating a Custom Policy**. The following section contains examples of common NAT Gateway custom policies.

Example Policies

- Example 1: Grant permissions to create and delete a NAT gateway.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "nat:natGateways:create",
                "nat:natGateways:delete"
            ]
        }
    ]
}
```

- Example 2: Grant permission to deny NAT gateway deletion.

  A policy with only "Deny" permissions must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the NAT Gateway **FullAccess** policy to a user but also forbid the user from deleting NAT gateways. Create a custom policy for denying NAT gateway deletion, and attach both policies to the group to which the user belongs. Then the user can perform all operations on NAT gateways except deleting NAT gateways. The following is an example of a deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "nat:natGateways:delete"
            ],
            "Effect": "Deny"
        }
    ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "nat:natGateways:update",
                "nat:natGateways:create"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:vpcs:update"
            ],
            "Effect": "Allow"
        }
    ]
}
```

4 Managing NAT Gateway Tags

Scenarios

A NAT gateway tag identifies the NAT gateway. Tags can be added to NAT gateways to ease NAT gateway identification and administration. You can add a tag to a NAT gateway when creating the NAT gateway. Alternatively, you can add a tag to a created NAT gateway on the NAT gateway details page. A maximum of ten tags can be added to each NAT gateway.

☐ **NOTE**

Only public NAT gateways support tag management.

A tag consists of a key and value pair. **Table 4-1** lists the tag key and value requirements.

Table 4-1 Tag requirements

Param eter	Requirement
Key	- Cannot be left blank. - Must be unique for each NAT gateway. - Can contain a maximum of 36 characters. - Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/), and the first and last characters cannot be spaces.
Value	- Can contain a maximum of 43 characters. - Cannot contain equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/), and the first and last characters cannot be spaces.

Procedure

Search for public NAT gateways by tag key or tag value on the page listing the public NAT gateways.

1. Log in to the management console.

2. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

3. In the upper right corner of the public NAT gateway list, click **Search by Tag**.

4. In the displayed area, enter the tag key and tag value of the public NAT gateway you are searching for. Both the tag key and value must be specified.

5. Click **+** to specify additional tag keys and values.

   You can add a maximum of ten tags to refine your search results. If you add more than one tag to search for public NAT gateways, the tags are automatically joined with AND.

6. Click **Search**.

   The system displays the public NAT gateways you are searching for based on the entered tag keys and tag values.

Add, delete, edit, and view tags of a public NAT gateway on the Tags tab.

1. Log in to the management console.

2. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

3. In the public NAT gateway list, locate the public NAT gateway whose tags you want to manage and click its name.

   The page showing details about the public NAT gateway is displayed.

4. Click the **Tags** tab and perform desired operations on tags.

   – View a tag.

      On the **Tags** tab, you can view tag details of the current public NAT gateway, including the number of tags and the key and value of each tag.

   – Add a tag.

      Click **Add Tag** in the upper left corner. In the displayed dialog box, enter the key and value of the tag to be added, and click **OK**.

      📖 **NOTE**

      You can use the predefined tags as prompted to simplify tag adding operations. For details, see **Predefined Tags**.

   – Modify a tag.

      Locate the row that contains the tag to be edited and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, change the tag value and click **OK**.

   – Delete a tag.

      Locate the row that contains the tag to be deleted and click **Delete** in the **Operation** column. In the displayed **Delete Tag** dialog box, click **Yes**.

5 Monitoring

5.1 Supported Metrics

Description

This section describes metrics reported by NAT Gateway to Cloud Eye as well as their namespaces, monitoring metrics, and dimensions. You can use the management console or the APIs provided by Cloud Eye to query the metrics generated for NAT Gateway.

Namespace

SYS.NAT

Metrics

Table 5-1 Public NAT gateway metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway Unit: count	≥ 0	Public NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bits/s	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
outbound_bandwidth	Outbound Bandwidth	Outbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bits/s	Public NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: count	≥ 0	Public NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: count	≥ 0	Public NAT gateway	1 minute
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Public NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Public NAT gateway	1 minute
snat_connection_ratio	SNAT Connection Usage	SNAT connection usage of the NAT gateway The maximum number of connections is the number of connections allowed by NAT gateway specifications. For details, see **NAT Gateway Specifications**. Unit: percent	≥ 0	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
inbound_bandwidth_ratio	Inbound Bandwidth Usage	Inbound bandwidth usage of servers using the SNAT function The maximum bandwidth supported by a public NAT gateway is 20 Gbit/s. Inbound bandwidth usage = Used bandwidth/Maximum bandwidth of the public NAT gateway x 100%. Unit: percent **NOTE** This metric is used to monitor the performance of public NAT gateways instead of the EIP bandwidth.	≥ 0	Public NAT gateway	1 minute
outbound_bandwidth_ratio	Outbound Bandwidth Usage	Outbound bandwidth usage of servers using the SNAT function The maximum bandwidth supported by a public NAT gateway is 20 Gbit/s. Outbound bandwidth usage = Used bandwidth/Maximum bandwidth of the public NAT gateway x 100%. Unit: percent **NOTE** This metric is used to monitor the performance of public NAT gateways instead of the EIP bandwidth.	≥ 0	Public NAT gateway	1 minute

Table 5-2 Private NAT gateway metrics

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway Unit: count	≥ 0	Private NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Inbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Private NAT gateway	1 minute
outbound_bandwidth	Outbound Bandwidth	Outbound bandwidth of servers using the SNAT function Unit: bit/s	≥ 0 bit/s	Private NAT gateway	1 minute
inbound_pps	Inbound PPS	Inbound PPS of servers using the SNAT function Unit: count	≥ 0	Private NAT gateway	1 minute
outbound_pps	Outbound PPS	Outbound PPS of servers using the SNAT function Unit: count	≥ 0	Private NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Monitored Object	Monitoring Period (Raw Data)
inbound_traffic	Inbound Traffic	Inbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute
outbound_traffic	Outbound Traffic	Outbound traffic of servers using the SNAT function Unit: byte	≥ 0 bytes	Private NAT gateway	1 minute

Dimensions

Key	Value
nat_gateway_id	Public NAT gateway ID
vpc_nat_gateway_id	Private NAT gateway ID

5.2 Creating Alarm Rules

Scenarios

You can set NAT gateway alarm rules to customize the monitored objects and notification policies. Then, you can learn NAT gateway running status in a timely manner.

Procedure

1. Log in to the management console.

2. Click in the upper left corner and select the desired region and project.

3. Under **Management & Governance**, select **Cloud Eye**.

4. In the left navigation pane, choose **Alarm Management** > **Alarm Rules**.

5. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters to create an alarm rule, or modify an existing alarm rule.

6. On the **Create Alarm Rule** page, follow the prompts to configure the parameters.

a. Set the alarm rule name and description.

Table 5-3 Configuring the alarm rule name and description

Parameter	Description
Name	Specifies the alarm rule name. The system generates a random name, which you can modify. Example value: **alarm-b6al**
Description	(Optional) Provides supplementary information about the alarm rule.

b. Select an object to be monitored and set alarm rule parameters.

Table 5-4 Parameters

Parameter	Description	Example Value
Resource Type	Specifies the type of the resource the alarm rule is created for.	NAT Gateway
Dimension	Specifies the metric dimension of the selected resource type.	Public NAT Gateway
Monitoring Scope	Specifies the monitoring scope the alarm rule applies to. You can select **Resource groups** or **Specific resources**. NOTE ● If **Resource groups** is selected and any resource in the group meets the alarm policy, an alarm is triggered. ● If you select **Specific resources**, select one or more resources and click ≫ to add them to the box on the right.	Specific resources
Method	There are two options: **Use template** or **Create manually**.	Create manually
Template	Specifies the template to be used. You can select a default alarm template or customize a template.	N/A

Parameter	Description	Example Value
Alarm Policy	Specifies the policy for triggering an alarm. If you set **Resource Type** to **Website Monitoring**, **Log Monitoring**, **Custom Monitoring**, or a specific cloud service, whether to trigger an alarm depends on whether the metric data in consecutive periods reaches the threshold. For example, Cloud Eye triggers an alarm if the raw data of the SNAT connections of the monitored object is 8000 or more for three consecutive 1-minute periods.	N/A
Alarm Severity	Specifies the alarm severity, which can be **Critical**, **Major**, **Minor**, or **Informational**.	Major

c. Configure the alarm notification.

Table 5-5 Alarm notification parameters

Parameter	Description
Alarm Notification	Specifies whether to notify users when alarms are triggered. Notifications can be sent by email, text message, or HTTP/HTTPS message.
Notification Object	Specifies the object to which alarm notifications will be sent. You can select the account contact or a topic. ● **Account contact**: Enter the phone number and email address of the registered account. ● A topic is used to publish messages and subscribe to notifications. If the required topic is unavailable, create one first and add subscriptions to it. For details, see the *Creating Alarm Notification Topics*.
Validity Period	Cloud Eye sends notifications only within the validity period specified in the alarm rule. If **Validity Period** is set to **08:00-20:00**, Cloud Eye sends notifications only within the time window.
Trigger Condition	Specifies the condition for triggering the alarm notification. You can select **Generated alarm** (when an alarm is generated), **Cleared alarm** (when an alarm is cleared), or both.

7. After the parameters are set, click **Create**.

After the alarm rule is set, the system automatically notifies you when an alarm is triggered.

> 📖 **NOTE**
>
> For more details, see **Alarm Rules**.

5.3 Viewing Metrics

Prerequisites

- The NAT gateway is running properly and SNAT rules have been created.
- It can take a period of time to obtain and transfer the monitoring data. Therefore, wait for a while and then check the data.
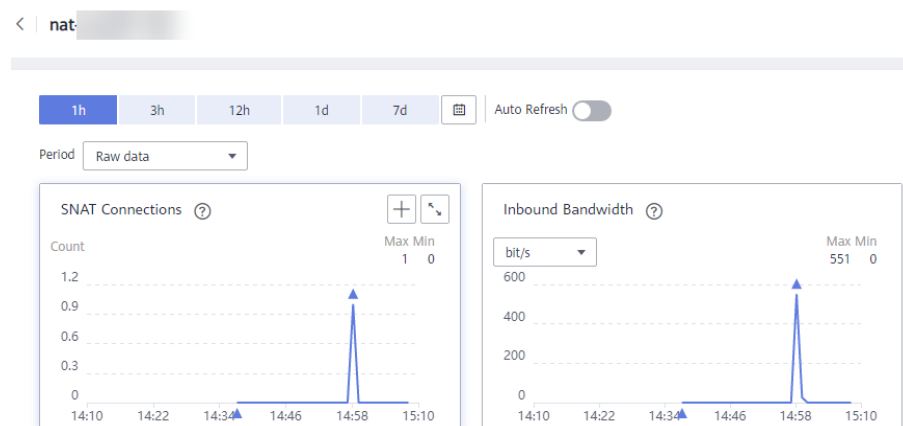
Scenarios

This section describes how to view NAT Gateway metrics.

Procedure

1. Log in to the management console.
2. In the upper left corner, select the target region.
3. Under **Management & Governance**, select **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **NAT Gateway**.
5. Locate the row that contains the target metric and click **View Metric** in the **Operation** column to check detailed information.

   You can view data of the last one, three, 12, or 24 hours, or last 7 days.

Figure 5-1 Viewing metrics

5.4 Viewing Metrics of Resources Using a NAT Gateway

Scenarios

You can view metrics details of resources using a specific NAT gateway. The resources can be ECSs or BMSs.

Procedure

1. Log in to the management console.

2. Click ⊙ in the upper left corner and select the desired region and project.

3. Click **Service List** in the upper left corner. Under **Networking**, select **NAT Gateway**.

   The NAT gateway console is displayed.

4. Click the name of the NAT gateway whose metrics you want to view.

5. On the displayed page, choose the **Monitoring** tab and click **View Details**.

   On the Cloud Eye console, view metrics of the NAT Gateway.

6. Configure a time range for metrics to be viewed.

7. Click ☰ in the upper right corner of the page to switch the display mode.

8. Select a metric to be viewed and click a specific time point in the displayed graph.

   In the lower part of the page, you can view the metric details of resources at the time point.

   Figure 5-2 Viewing metrics
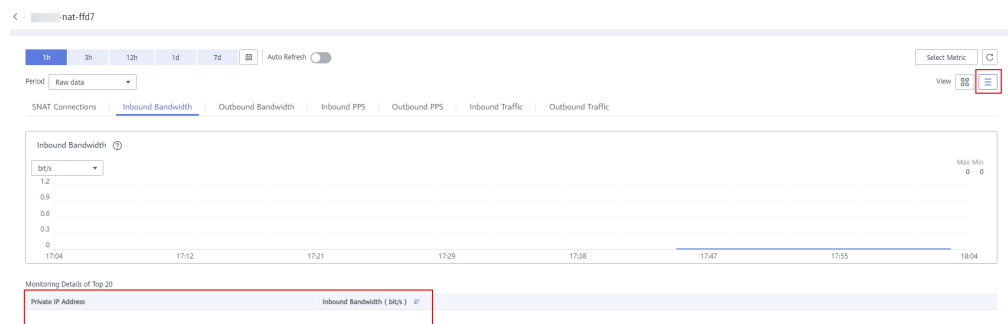
6 Auditing

6.1 Key Operations Recorded by CTS

You can use CTS to record operations on NAT Gateway for query, auditing, and backtracking.

Table 6-1 lists public NAT gateway operations that can be recorded by CTS.

Table 6-1 Public NAT gateway operations

Operation	Resource Type	Trace
Creating a public NAT gateway	natgateway	createNatGateway
Modifying a public NAT gateway	natgateway	updateNatGateway
Deleting a public NAT gateway	natgateway	deleteNatGateway
Creating a DNAT rule	dnatrule	createDnatRule
Modifying a DNAT rule	dnatrule	updateDnatRule
Deleting a DNAT rule	dnatrule	deleteDnatRule
Creating an SNAT rule	snatrule	createSnatRule
Modifying an SNAT rule	snatrule	updateSnatRule
Deleting an SNAT rule	snatrule	deleteSnatRule

6.2 Viewing Traces

Scenarios

CTS records the operations performed on NAT Gateway and allows you to view the operation records of the last seven days on the CTS console. This topic describes how to query these records.

Procedure

1. Log in to the management console.

2. In the upper left corner of the page, click ⊙ and select the desired region and project.

3. Under **Management & Governance**, click **Cloud Trace Service**.

4. In the navigation pane on the left, choose **Trace List**.

5. Specify the filters used for querying traces. The following filters are available:

   – **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

   Select a filter from the drop-down list.

   If you select **Trace name** for **Search By**, select a specific trace name.

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

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

   – **Operator**: Select a specific operator (at the user level rather than the tenant level).

   – **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.

   – Time range: You can query traces generated at any time range of the last seven days.

6. Click ⌄ on the left of the required trace to expand its details.

   Figure 6-1 Expanding trace details
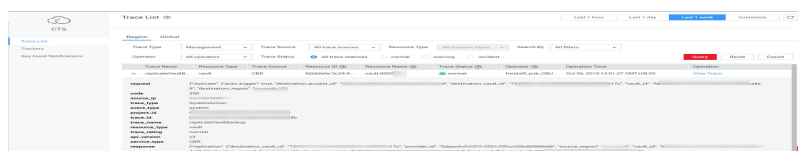
7. Click **View Trace** in the **Operation** column to view trace details.

Figure 6-2 View Trace

```
"context": {
    "code": "204",
    "source_ip": "10.45.152.59",
    "trace_type": "ApiCall",
    "event_type": "system",
    "project_id": "0503dda897000fed2f78c00909158a4d",
    "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\": \"0503dda897000fed2f78c00909158a4d\", \"name\": \"9646e73b-338c-
    "resource_id": "
    "tracker_name": "system",
    "time": "1569321775225",
    "resource_name": "9646e73b-338c-4d27-a17c-219be532812c",
    "record_time": "1569321775903",
    "user": {
        "domain": {
            "name": "
            "id": "0503dda878000fed0f75c0096d70a960"
        },
```

For details about key fields in the trace, see section "Trace Structure" in *Cloud Trace Service User Guide*.