

# NAT Gateway

# User Guide

**Issue** 01  
**Date** 2026-03-27



**Copyright © Huawei Technologies Co., Ltd. 2026. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## **Huawei Technologies Co., Ltd.**

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <https://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

# Security Declaration

## Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

# Contents

<b>1 Using IAM to Grant Access to NAT Gateway.....</b>	<b>1</b>
1.1 Creating a User and Granting NAT Gateway Permissions.....	1
1.2 NAT Gateway Custom Policies.....	2
<b>2 Public NAT Gateways.....</b>	<b>5</b>
2.1 Overview of Public NAT Gateways.....	5
2.2 Buying a Public NAT Gateway.....	6
2.3 Managing Public NAT Gateways.....	10
2.4 Managing SNAT Rules.....	11
2.4.1 Adding an SNAT Rule.....	11
2.4.2 Modifying an SNAT Rule.....	13
2.4.3 Deleting an SNAT Rule.....	14
2.5 Managing DNAT Rules.....	14
2.5.1 Adding a DNAT Rule.....	14
2.5.2 Modifying a DNAT Rule.....	17
2.5.3 Deleting a DNAT Rule.....	17
2.5.4 Deleting DNAT Rules in Batches.....	18
2.5.5 Importing DNAT Rules by Using a Template and Exporting DNAT Rules .....	18
<b>3 Private NAT Gateways.....</b>	<b>21</b>
3.1 Overview of Private NAT Gateways.....	21
3.2 Buying a Private NAT Gateway.....	24
3.3 Managing Private NAT Gateways.....	26
3.4 Managing SNAT Rules.....	27
3.4.1 Adding an SNAT Rule.....	27
3.4.2 Modifying an SNAT Rule.....	28
3.4.3 Deleting an SNAT Rule.....	28
3.5 Managing DNAT Rules.....	29
3.5.1 Adding a DNAT Rule.....	29
3.5.2 Modifying a DNAT Rule.....	31
3.5.3 Deleting a DNAT Rule.....	32
3.6 Managing Transit IP Addresses.....	32
3.6.1 Assigning a Transit IP Address.....	32
3.6.2 Viewing a Transit IP Address.....	34

---

3.6.3 Releasing a Transit IP Address.....	34
<b>4 Managing NAT Gateway Tags.....</b>	<b>35</b>
<b>5 Managing Quotas.....</b>	<b>37</b>
<b>6 Monitoring.....</b>	<b>39</b>
6.1 Monitoring NAT Gateway Resources.....	39
6.2 NAT Gateway Monitoring Metrics.....	39
<b>7 Auditing.....</b>	<b>46</b>
7.1 Key Operations Recorded by CTS.....	46
7.2 Viewing Traces.....	49

# 1 Using IAM to Grant Access to NAT Gateway

---

[1.1 Creating a User and Granting NAT Gateway Permissions](#)

[1.2 NAT Gateway Custom Policies](#)

## 1.1 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 a 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.

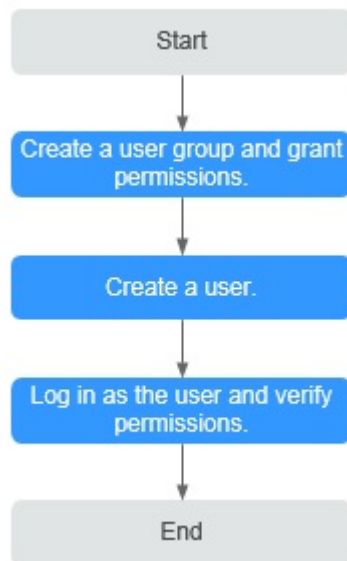
This section describes the procedure for granting permissions (see [Figure 1-1](#)).

### 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 1-1 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 **NATReadOnlyAccess** 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 **NATReadOnlyAccess** 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 **NATReadOnlyAccess** policy has already taken effect.

## 1.2 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. This does not require knowledge of 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 permissions 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: Define 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"
    }
  ]
}
```



# 2 Public NAT Gateways

---

[2.1 Overview of Public NAT Gateways](#)

[2.2 Buying a Public NAT Gateway](#)

[2.3 Managing Public NAT Gateways](#)

[2.4 Managing SNAT Rules](#)

[2.5 Managing DNAT Rules](#)

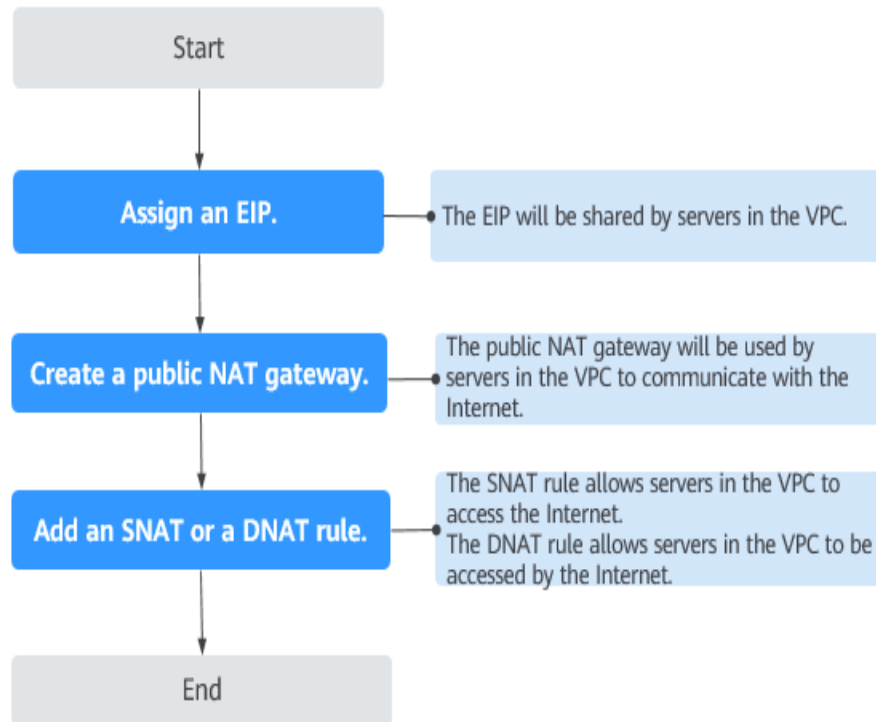
## 2.1 Overview of Public NAT Gateways

Public NAT gateways provide network address translation (NAT) with 20 Gbit/s of bandwidth for servers in a VPC or for servers in on-premises data centers that connect to a VPC through Direct Connect or VPN.

Public NAT gateways allow multiple servers to share an EIP to access the Internet or to provide services accessible from the Internet.

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

**Figure 2-1** Process of using a public NAT gateway



## 2.2 Buying a Public NAT Gateway

### Scenarios

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

### Constraints

- Rules on a 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.
- Only one NAT gateway can be created for a subnet.
- SNAT and DNAT rules can use the same EIP to save resources. However, when **Port Type** of a DNAT rule is set to **All ports**, the resources configured for the DNAT rule will preferentially use all ports of the EIP. So an SNAT rule cannot share an EIP with such a DNAT rule.
- A 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 ports shown below table.

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 create 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 route table already has a route with the destination of 0.0.0.0/0, the default route that points to the public NAT gateway will fail to be added. In this case, manually add a route that points to the gateway or create a custom route table and add a route with the destination of 0.0.0.0/0 pointing to the gateway to the new route table.

## Procedure

1. Go to the [Buy Public NAT Gateway](#) page.
2. Configure required parameters. For details, see [Table 2-1](#).

**Table 2-1** Descriptions of public NAT gateway parameters

Parameter	Description
Region	The region where the public NAT gateway is located.
Billing Mode	Public NAT gateways are billed on a pay-per-use or yearly/monthly basis.
Specifications	The specifications of the public NAT gateway. The value can be <b>Small</b> , <b>Medium</b> , <b>Large</b> , or <b>Extra-large</b> . You can click <b>Learn more</b> on the page to view details of each specification.
Name	The name of the public NAT gateway. Enter up to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.

Parameter	Description
VPC	<p>The VPC that the public NAT gateway belongs to. The selected VPC cannot be changed after the public NAT gateway is purchased.</p> <p><b>NOTE</b> 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 route table already has a route with the destination of 0.0.0.0/0, the default route that points to the public NAT gateway will fail to be added. In this case, manually add a route that points to the gateway or create a custom route table and add a route with the destination of 0.0.0.0/0 pointing to the gateway to the new route table.</p>
Subnet	<p>The subnet that the public NAT gateway belongs to.</p> <p>The subnet must have at least one available IP address.</p> <p>The selected subnet cannot be changed after the public NAT gateway is purchased.</p> <p>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.</p>
Enterprise Project	<p>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 <b>default</b> enterprise project.</p>
Advanced Settings (Optional)	<p>Click the drop-down arrow to configure advanced parameters of the public NAT gateway, such as <b>Description</b>.</p>
SNAT Connection TCP Timeout (s)	<p>The timeout period of a TCP connection established using the SNAT rule. If no data is exchanged within this period, the TCP connection will be closed.</p> <p>Value range: 40 to 7200</p>
SNAT Connection UDP Timeout (s)	<p>The timeout period of a UDP connection established using the SNAT rule. If no data is exchanged within this period, the UDP connection will be closed.</p> <p>Value range: 40 to 7200</p>

Parameter	Description
SNAT Connection ICMP Timeout (s)	The timeout period of an ICMP connection established using the SNAT rule. If no data is exchanged within this period, the ICMP connection will be closed. Value range: 10 to 7200
TCP TIME_WAIT (s)	How long the side that actively closed the TCP connection is in the <b>TIME_WAIT</b> state. Value range: 0 to 1800
Description	Supplementary information about the public NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.
Tag	The identifier of the public NAT gateway. A tag is a key-value pair. You can add up to 20 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 <a href="#">Table 2-2</a> .

**Table 2-2** Tag requirements

Parameter	Requirement
Key	<ul style="list-style-type: none"> <li>Cannot be left blank.</li> <li>Must be unique for each NAT gateway.</li> <li>Can contain a maximum of 36 characters.</li> <li>Cannot contain equal signs (=), asterisks (*), left angle brackets (&lt;), right angle brackets (&gt;), backslashes (\), commas (,), vertical bars ( ), and slashes (/), and cannot start or end with spaces.</li> </ul>
Value	<ul style="list-style-type: none"> <li>Can contain a maximum of 43 characters.</li> <li>Cannot contain equal signs (=), asterisks (*), left angle brackets (&lt;), right angle brackets (&gt;), backslashes (\), commas (,), vertical bars ( ), and slashes (/), and cannot start or end with spaces.</li> </ul>

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

4. Click **Submit**.  
The creation takes 1 to 5 minutes to complete.
5. In the public NAT gateway list, you can see the gateway status.

 **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 created. 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. For details, see [Adding Routes to a Route Table](#).

## FAQ

### What Should I Do If the Number of NAT Gateway Connections Exceeds the Upper Limit?

- If the number of connections goes beyond the number defined in each public NAT gateway specification, packets will be dropped. To avoid this, create alarm rules on the Cloud Eye console to monitor the number of SNAT connections.
- If the number of requests exceeds the maximum allowed connections of a NAT gateway, you are advised to upgrade the specifications of the NAT gateway by referring to [2.3 Managing Public NAT Gateways](#).

### Does Changing NAT Gateway Specifications Interrupt Services?

If you downgrade a NAT gateway, make sure that the new specification can meet your service requirements.

## 2.3 Managing Public NAT Gateways

### Scenarios

After a public NAT gateway is created, you can modify the name, specifications, or description of it. You can also delete or unsubscribe from public NAT gateways that are no longer needed to release resources and reduce costs.

If you downgrade a NAT gateway, make sure that the new specification can meet your service requirements.

Upgrading a NAT gateway does not affect services.

### Modifying a Public NAT Gateway

1. Go to the [public NAT gateway list](#) page.
2. Locate the public NAT gateway you want to modify and click **Modify** in the **Operation** column.
3. Modify the name, specifications, and description of the public NAT gateway.

**Figure 2-2** Modifying a NAT gateway

< Change Specifications

**Note**  
After the NAT gateway specifications are changed, the NAT gateway is billed based on the highest specifications applied on that day.

**Current Configuration**

Name nat-0105 Region [dropdown]  
ID 8/... db Specifications Small  
Description -- Billing Mode [dropdown]

**New Configuration**

Name nat-0105  
Specifications Small Medium Large Extra-large  
Supports up to 50,000 connections. [Learn more](#)

Advanced Settings  
SNAT Connection TCP Timeout (s): 900 SNAT Connection UDP Timeout (s): 300 SNAT Connection ICMP Timeout (s): 10 TCP TIME\_WAIT (s): 5 Description: --

4. After the modification is complete, click **Next**, view the comparison information, and click **Submit**. You can view the information about the modified NAT gateway in the public NAT gateway list.

## Deleting or Unsubscribing from a Public NAT Gateway

1. Go to the [public NAT gateway list](#) page.
2. On the displayed page, locate the public NAT gateway that you want to delete and choose **More > Delete** in the **Operation** column.
3. In the displayed dialog box, enter **DELETE**.
4. Click **OK**.

## 2.4 Managing SNAT Rules

### 2.4.1 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, add multiple SNAT rules to allow servers in the subnets to share an EIP.

#### Constraints

- Only one SNAT rule can be added for each VPC subnet.
- If an SNAT rule is added for a Direct Connect connection, the custom CIDR block must be the CIDR block of a Direct Connect connection and cannot overlap with that of NAT gateway's VPC.

- There is no limit on the number of SNAT rules that can be added on a public NAT gateway.

## Adding an SNAT Rule

1. Go to the [public NAT gateway list](#) page.
2. On the displayed page, click the name of the public NAT gateway on which you need to add an SNAT rule.
3. On the **SNAT Rules** tab, click **Add SNAT Rule**.

Figure 2-3 Add SNAT Rule

**Add SNAT Rule**

**Public NAT Gateway Name**  
nat-ab44

**Scenario**  
VPC Direct Connect/Cloud Connect

**CIDR Block**  
Existing Custom

st

**Public IP Address Type**  
EIP

You can select 20 more EIPs. [View EIP](#)

Select a property or enter a keyword.

<input type="checkbox"/>	EIP	EIP Type	Bandwidth Name	Bandwidth (Mbit/s)	Billing Mode	Enterprise Project
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						
<input type="checkbox"/>						

Total Records: 21

[If multiple EIPs are selected for an SNAT rule, the system picks one at random to provide services accessible from the Internet.](#)

Monitoring

Cancel OK

4. Configure required parameters. For details, see [Table 2-3](#).

**Table 2-3** Descriptions of SNAT rule parameters

Parameter	Description
Scenario	The scenarios where the SNAT rule is used Select <b>VPC</b> if your servers in a VPC need to access the Internet. Select <b>Direct Connect/Cloud Connect</b> if servers in your on-premises data center or in another VPC need to access the Internet.
CIDR Block	In a VPC scenario, specify a VPC subnet to enable servers in that subnet to access the Internet using the SNAT rule. In a Direct Connect/Cloud Connect scenario, specify a CIDR block of your data center or your VPC to enable your servers to access the Internet using the SNAT rule.
Public IP Address Type	The type of the public IP address used for accessing the Internet <b>EIP</b> : You can select an EIP that has not been bound to any resource or has been bound to an SNAT rule in the current VPC.
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.

5. Click **OK**.

## 2.4.2 Modifying an SNAT Rule

### Scenarios

After an SNAT rule is added, you can modify parameters in the SNAT rule as required.

Note that modifying an SNAT rule may interrupt your services.

### Prerequisites

An SNAT rule has been added.

### Procedure

1. Go to the [public NAT gateway list](#) page.
2. Click the name of the public NAT gateway.
3. On the **SNAT Rules** tab, locate the SNAT rule you want to modify.

4. Click **Modify** in the **Operation** column.
5. In the displayed dialog box, modify the type of the public IP address or description.
6. Click **OK**.

## 2.4.3 Deleting an SNAT Rule

### Scenarios

You can delete SNAT rules that are no longer needed.

### Prerequisites

An SNAT rule has been added.

### Procedure

1. Go to the [public NAT gateway list](#) page.
2. Click the name of the public NAT gateway.
3. In the SNAT rule list, locate the SNAT rule you want to delete and click **Delete** in the **Operation** column.
4. Enter **DELETE** in the displayed dialog box and click **OK**.

## 2.5 Managing DNAT Rules

### 2.5.1 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.

#### Constraints

- 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, add multiple DNAT rules.
- A maximum of 200 DNAT rules can be added on a public NAT gateway.

#### Procedure

1. Go to the [public NAT gateway list](#) page.
2. On the displayed page, click the name of the public NAT gateway on which you need to add a DNAT rule.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. Click **Add DNAT Rule**.

**Figure 2-4** Add DNAT Rule

**Add DNAT Rule** ✕

**Warning:**

- If your server 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](#)
- Add security group rules to allow inbound or outbound traffic after you add a DNAT rule. [Manage security group rules](#)
- It is not recommended that an SNAT rule and a DNAT rule share the same EIP because there may be service conflicts.
- An SNAT rule cannot share an EIP with a DNAT rule with Port Type set to All ports.

Public NAT Gateway Name:

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

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

\* Protocol: TCP

\* Public IP Address Type: **EIP**

Public Port: --Select-- [View EIP](#)

\* Instance Type: Server Virtual IP address **Custom**

\* Private IP Address:

\* Private Port: Example: 22 or 22-30

Description:

Cancel **OK**

5. Configure required parameters. For details, see [Table 2-4](#).

**Table 2-4** Descriptions of DNAT rule parameters

Parameter	Description
Scenario	<p>Select <b>VPC</b> if your servers in a VPC will use the DNAT rule to share the same EIP to provide services accessible from the Internet.</p> <p><b>Direct Connect/Cloud Connect:</b> 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.</p>
Port Type	<p>The port type.</p> <ul style="list-style-type: none"> <li>• <b>All ports:</b> The public NAT gateway directs all requests received by the EIP to the private IP address of the destination cloud server.</li> <li>• <b>Specific port:</b> The public NAT gateway forwards requests intended for the EIP over specified ports and protocol to specified ports of the destination cloud server.</li> </ul>

Parameter	Description
Protocol	The protocol can be TCP or UDP. This parameter is available if you select <b>Specific port</b> for <b>Port Type</b> . If you select <b>All ports</b> , the value of this parameter is <b>All</b> by default.
Public IP Address Type	The type of the public IP address used for accessing the Internet. <b>EIP:</b> You can select an EIP that has not been bound to any resource or has been bound to a DNAT rule in the current VPC.
Public Port	The port of the EIP used by the NAT gateway for external communications. This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> . 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: <ul style="list-style-type: none"> <li>• <b>Server</b></li> <li>• <b>Virtual IP address</b></li> <li>• <b>Custom</b></li> </ul>
NIC	The NIC of the server. This parameter is available if you set <b>Instance Type</b> to <b>Server</b> .
Private IP Address	<ul style="list-style-type: none"> <li>• In a VPC scenario, this parameter can only be set 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.</li> <li>• In a Direct Connect/Cloud Connect scenario, set this parameter to the 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.</li> <li>• Configure the port of <b>Private IP Address</b> if you select <b>Specific port</b> for <b>Port Type</b>.</li> </ul>
Private Port	The port of the server over which the originating requests will be forwarded. This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> . Range: 1 to 65535 You can enter a specific port number or a port range, for example, 80 or 80-100.

Parameter	Description
Description	Provides supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

- 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 will not work.

## 2.5.2 Modifying a DNAT Rule

### Scenarios

After a DNAT rule is added, you can modify parameters in the DNAT rule as required.

Note that modifying a DNAT rule may interrupt your services.

### Prerequisites

A DNAT rule has been added.

### Procedure

- Go to the [public NAT gateway list](#) page.
- Click the name of the public NAT gateway.
- On the public NAT gateway details page, click the **DNAT Rules** tab.
- In the DNAT rule list, locate the DNAT rule you want to modify and click **Modify** in the **Operation** column.
- In the displayed dialog box, modify parameters as needed.
- Click **OK**.

## 2.5.3 Deleting a DNAT Rule

### Scenarios

You can delete DNAT rules that are no longer needed.

### Prerequisites

A DNAT rule has been added.

## Procedure

1. Go to the [public NAT gateway list](#) page.
2. Click the name of the public NAT gateway.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, locate the DNAT rule you want to delete and click **Delete** in the **Operation** column.
5. Enter **DELETE** in the displayed dialog box and click **OK**.

## 2.5.4 Deleting DNAT Rules in Batches

### Scenarios

Delete DNAT rules that you no longer need.

### Prerequisites

DNAT rules have been added.

## Procedure

1. Go to the [public NAT gateway list](#) page.
2. Click the name of the public NAT gateway.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, select the DNAT rules that you no longer need and click **Delete DNAT Rule**.
5. In the displayed dialog box, click **OK**.

## 2.5.5 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.

### Importing DNAT Rules

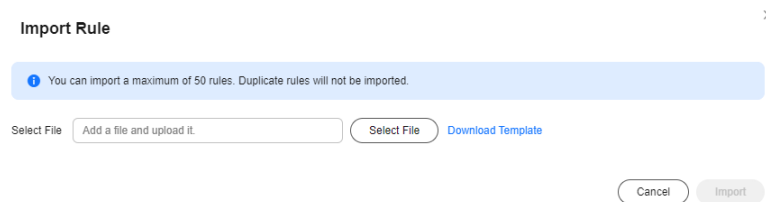
1. Go to the [public NAT gateway list](#) page.
2. On the displayed page, click the name of the public NAT gateway to which you want to import DNAT rules.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. On the displayed page, click **Import**. In the displayed **Import Rule** dialog box, click **Download Template**.
5. Fill in DNAT rule parameters based on the table heading in the template. For details, see [Table 2-5](#).

**Table 2-5** Descriptions of DNAT rule parameters

Parameter	Description
Scenario	<p>The following two scenarios are available:</p> <ul style="list-style-type: none"> <li>• <b>VPC:</b> The servers in a VPC will share an EIP to provide services accessible from the Internet through the DNAT rule.</li> <li>• <b>Direct Connect/Cloud Connect:</b> 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.</li> </ul>
Protocol	The value can be <b>TCP</b> , <b>UDP</b> , or <b>All</b> .
EIP	<p>The EIP that will be used by the server to provide publicly accessible services</p> <p>Only idle EIPs or EIPs that have been bound to a DNAT rule in the current VPC are available for selection.</p>
Public Port	<p>The EIP port</p> <p>This parameter is only available if <b>Specific port</b> is selected for <b>Port Type</b>.</p> <p>You can enter a specific port number or a port range, for example, 80 or 80-100.</p>
Private IP Address	<ul style="list-style-type: none"> <li>• 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.</li> <li>• In a Direct Connect/Cloud Connect scenario, set this parameter to the 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.</li> <li>• Configure the private IP address port if <b>Protocol</b> is set to <b>TCP</b> or <b>UDP</b>.</li> </ul>
Private Port	<ul style="list-style-type: none"> <li>• In a VPC scenario, set this parameter to the port of the server in a VPC.</li> <li>• 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.</li> <li>• This parameter is only available if <b>Specific port</b> is selected for <b>Port Type</b>.</li> </ul> <p>The number of private and public ports must match.</p>
Description	Supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

6. After filling in the template, click **Add**, select the local template, and click **Import**.

**Figure 2-5** Import Rule



7. View the imported DNAT rules.  
If their status is **Running**, the DNAT rules have been imported.

## Exporting DNAT Rules

1. Go to the [public NAT gateway list](#) page.
2. On the displayed page, click the name of the public NAT gateway from which you want to export DNAT rules.
3. On the public NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list page, click **Export**.
  - a. **Export all data to an XLSX file:** The system automatically exports the basic information of all the DNAT rules in the current region as an Excel file to a local directory.
  - b. **Export selected data to an XLSX file:** The system automatically exports the basic information of the selected DNAT rules in the current region as an Excel file to a local directory.

# 3 Private NAT Gateways

---

- [3.1 Overview of Private NAT Gateways](#)
- [3.2 Buying a Private NAT Gateway](#)
- [3.3 Managing Private NAT Gateways](#)
- [3.4 Managing SNAT Rules](#)
- [3.5 Managing DNAT Rules](#)
- [3.6 Managing Transit IP Addresses](#)

## 3.1 Overview of Private NAT Gateways

### Private NAT Gateways

Private NAT gateways provide private address translation (NAT) for cloud servers (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 a VPC can communicate with other VPCs or on-premises data centers.

Specifically:

- SNAT enables servers in a VPC, regardless of whether they are in the same AZ, to share a transit IP address to access on-premises data centers or other VPCs.
- DNAT enables servers in a VPC, regardless of whether they are in the same AZ, to share a transit IP address to provide services accessible from on-premises data centers or other VPCs.

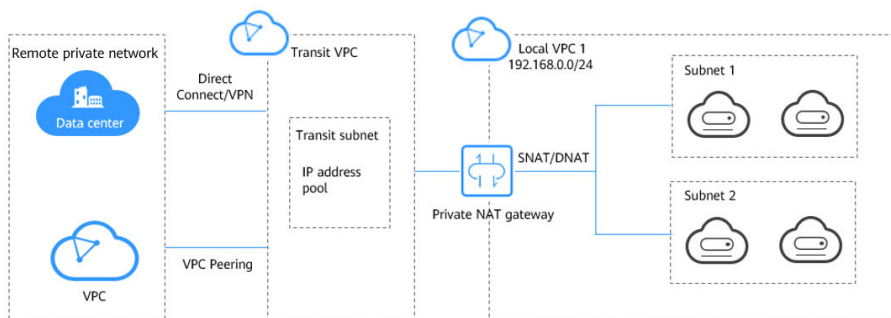
#### Transit Subnet

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

A transit VPC is where a transit subnet is created.

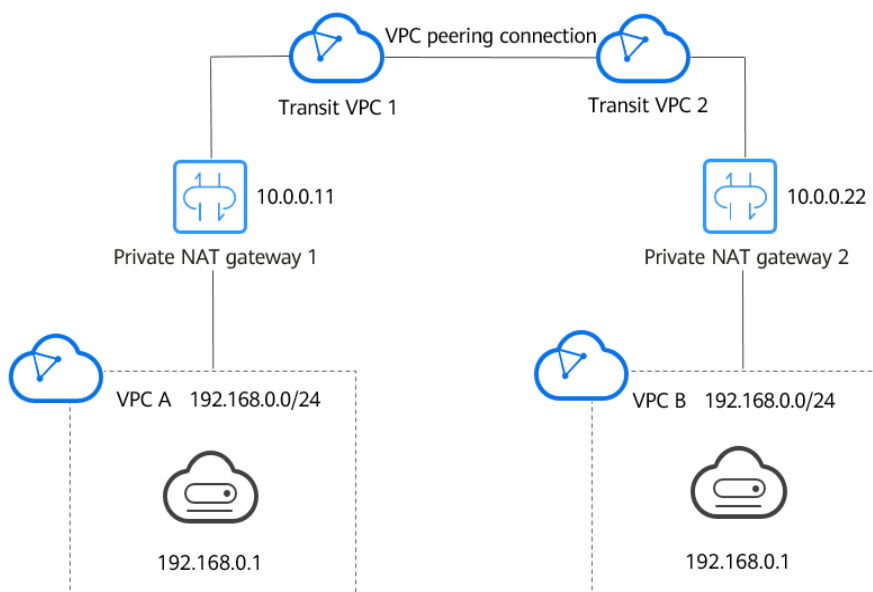
**Figure 3-1** Private NAT gateway



## Application Scenarios

- Connecting VPCs with overlapping CIDR blocks  
You can configure two private NAT gateways for two VPCs with overlapping CIDR blocks. Then, add SNAT and DNAT rules on the two private NAT gateways to enable servers in the two VPCs to use the transit IP addresses to communicate with each other.

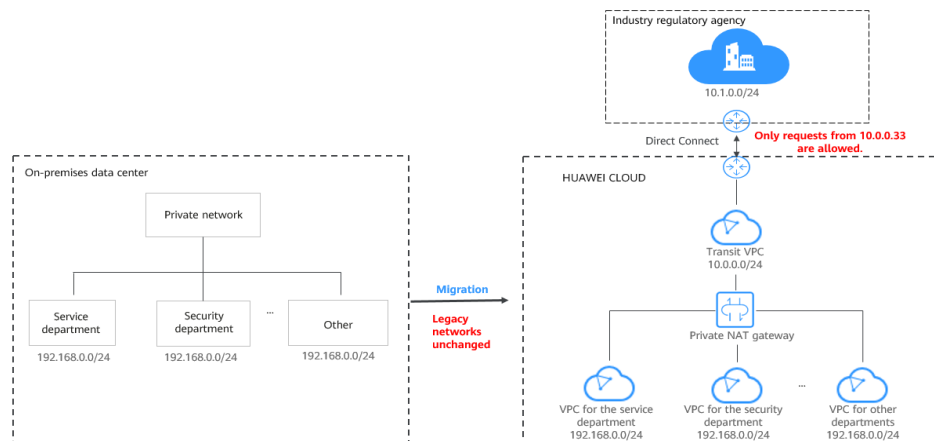
**Figure 3-2** Connecting VPCs with overlapping CIDR blocks



- Migrating workloads to the cloud without changing the network topology or accessing regulatory agencies from specific IP addresses  
Organizations may want to migrate their workloads to the cloud without making any changes to their existing network topology. They may also have to access regulatory agencies from specific IP addresses as required by these agencies. A private NAT gateway is a good choice.  
The following figure represents an enterprise network where the subnets of different departments overlap. A private NAT gateway allows the enterprise to keep the existing network topology unchanged while migrating their workloads to the cloud. In this example, the private NAT gateway maps the IP

address of each department to 10.0.0.33 so that each department can use 10.0.0.33 to securely access the regulatory agency.

**Figure 3-3** Migrating workloads to the cloud and accessing regulatory agencies from specific IP addresses



## 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 share a transit IP address to 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 3-1** describes the differences between public and private NAT gateways.

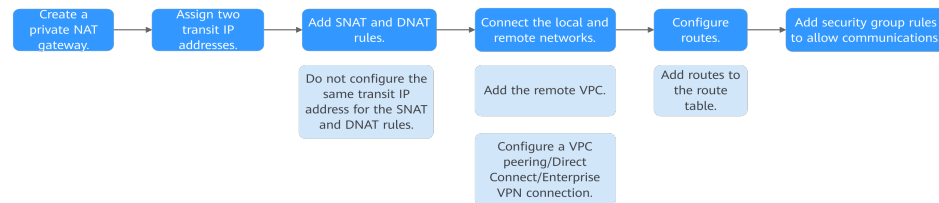
**Table 3-1** Differences between public and private NAT gateways

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.
IP type for communication	EIP	Transit IP address

## Process for Deploying a Private NAT Gateway

The below figure shows the process for deploying a private NAT gateway.

**Figure 3-4** Process for deploying a private NAT gateway



## 3.2 Buying a Private NAT Gateway

### Scenarios

You need 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

- You need to manually add routes to a VPC route table to connect it to a remote private network through a VPC peering connection, Direct Connect, or VPN connection.
- 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. Go to the [Buy Private NAT Gateway](#) page.
2. Configure required parameters. For details, see [Table 3-2](#).

**Table 3-2** Descriptions of private NAT gateway parameters

Parameter	Description
Billing Mode	Private NAT gateways can be billed on a pay-per-use basis.

Parameter	Description
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 <b>Extra-large</b> , <b>Large</b> , <b>Medium</b> , or <b>Small</b> . For details about specifications, see <a href="#">NAT Gateway Specifications</a> .
Enterprise Project	The enterprise project that the private 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 <b>default</b> enterprise project.
Tag	The private NAT gateway tag. A tag is a key-value pair. You can add up to 20 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 <a href="#">Table 3-3</a> .
Description	Supplementary information about the private NAT gateway. Enter up to 255 characters. Angle brackets (<>) are not allowed.

**Table 3-3** Tag requirements

Parameter	Requirement
Key	<ul style="list-style-type: none"><li>• Cannot be left blank.</li><li>• Must be unique for each NAT gateway.</li><li>• Can contain a maximum of 36 characters.</li><li>• Cannot contain equal signs (=), asterisks (*), left angle brackets (&lt;), right angle brackets (&gt;), backslashes (\), commas (,), vertical bars ( ), and slashes (/), and cannot start or end with spaces.</li></ul>
Value	<ul style="list-style-type: none"><li>• Can contain a maximum of 43 characters.</li><li>• Cannot contain equal signs (=), asterisks (*), left angle brackets (&lt;), right angle brackets (&gt;), backslashes (\), commas (,), vertical bars ( ), and slashes (/), and cannot start or end with spaces.</li></ul>

3. Click **Buy Now**.

## Other Operations

- [3.6.1 Assigning a Transit IP Address](#)
- [3.4.1 Adding an SNAT Rule](#)
- [3.5.1 Adding a DNAT Rule](#)
- [Managing Private NAT Gateways](#)

## 3.3 Managing Private NAT Gateways

After a private NAT gateway is created, you can manage it in a unified manner, including modifying and deleting the private NAT gateway.

### Modifying a Private NAT Gateway

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

1. Go to the [private NAT gateway list](#) page.
2. On the displayed page, locate the private NAT gateway you want to modify and click **Modify** in the **Operation** column.
3. Modify the name, specifications, and description of the private NAT gateway.
4. Click **Next**.
5. Confirm the modification and click **Submit**.

### Deleting a Private NAT Gateway

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

 **NOTE**

Before deleting a private NAT gateway, ensure all SNAT and DNAT rules on it have been deleted. For details about how to delete SNAT and DNAT rules, see [Deleting an SNAT Rule](#) and [Deleting a DNAT Rule](#).

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, locate the private NAT gateway that you want to delete and click **Delete** in the **Operation** column.
3. In the displayed dialog box, enter **DELETE**.
4. Click **OK**.

## 3.4 Managing SNAT Rules

### 3.4.1 Adding an SNAT Rule

#### Scenarios

After a 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 an on-premises data center or another VPC.

#### Notes and Constraints

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

#### Prerequisites

- A private NAT gateway is available.
- A transit IP address is 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. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add an SNAT rule.
3. On the **SNAT Rules** tab, click **Add SNAT Rule**.
4. Configure required parameters. For details, see [Table 3-4](#).

**Table 3-4** Parameter descriptions of an SNAT rule

Parameter	Description
Subnet	The subnet type of the SNAT rule. Select <b>Existing</b> or <b>Custom</b> . Select a subnet where IP address translation is required in the service VPC.

Parameter	Description
Monitoring	You can create alarm rules using Cloud Eye after your SNAT connection has been created.
Transit IP Address	The transit IP address used to access on-premises data centers or other VPCs.
Description	Provides supplementary information about the SNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

- Click **OK**.

 **NOTE**

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

## Helpful Links

### [3.4 Managing SNAT Rules](#)

## 3.4.2 Modifying an SNAT Rule

### Scenarios

After an SNAT rule is added, you can modify parameters in the SNAT rule as required.

Note that modifying an SNAT rule may interrupt your services.

### Prerequisites

An SNAT rule has been added.

### Procedure

- Go to the [private NAT gateway list](#) page.
- On the **Private NAT Gateways** page, click the name of the private NAT gateway.
- On the **SNAT Rules** tab, locate the SNAT rule you want to modify.
- Click **Modify** in the **Operation** column.
- In the displayed dialog box, modify the transit IP address and description of the SNAT rule.
- Click **OK**.

## 3.4.3 Deleting an SNAT Rule

### Scenarios

You can delete SNAT rules that are no longer needed.

## Prerequisites

An SNAT rule has been added.

## Procedure

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
3. In the SNAT rule list, locate the SNAT rule you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **OK**.

# 3.5 Managing DNAT Rules

## 3.5.1 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 accessed. 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

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.
- A transit IP address is available.

### Procedure

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click the name of the private NAT gateway on which you need to add a DNAT rule.
3. On the private NAT gateway details page, click the **DNAT Rules** tab.
4. Click **Add DNAT Rule**.

**NOTICE**

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

5. Configure required parameters. For details, see [Table 3-5](#).

**Table 3-5** Descriptions of DNAT rule parameters

Parameter	Description
<b>Local Network</b>	
Port Type	<p>The port type.</p> <p>The type can be:</p> <ul style="list-style-type: none"> <li>• <b>Specific port:</b> The private NAT gateway forwards requests intended for the transit IP address over the specified port and protocol to the specified port of the destination cloud server.</li> <li>• <b>All ports:</b> The private NAT gateway directs all requests received by the transit IP address to the private IP address of the destination cloud server.</li> </ul>
Protocol	<p>The protocol can be TCP or UDP.</p> <p>If you select <b>All ports</b>, the value of this parameter is <b>All</b> by default.</p> <p>This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b>.</p>
Instance Type	<p>The type of instance that will provide services accessible from on-premises data centers or other VPCs.</p> <p>Possible types are:</p> <ul style="list-style-type: none"> <li>• <b>Server</b></li> <li>• <b>Virtual IP address</b></li> <li>• <b>Load balancer</b></li> <li>• <b>Custom</b></li> </ul>
NIC	<p>The NIC of the server.</p> <p>This parameter is only available if you set <b>Instance Type</b> to <b>Server</b>.</p>
IP Address	<p>The IP address of the server that will provide services accessible from on-premises data centers or other VPCs.</p> <p>This parameter is only available if you set <b>Instance Type</b> to <b>Custom</b>.</p>

Parameter	Description
Internal Port	The port used by the instance to provide services accessible from on-premises data centers or other VPCs. Range: 1 to 65535 This parameter is only available if you select <b>Specific port</b> for <b>Port Type</b> .
<b>Transit Network</b>	
Transit IP Address	The transit IP address used to provide services accessible from 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 <b>Port Type</b> is set to <b>Specific port</b> , or has been bound to an 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 <b>Specific port</b> for <b>Port Type</b> .
Description	Supplementary information about the DNAT rule. Enter up to 255 characters. Angle brackets (<>) are not allowed.

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

## Helpful Links

### [3.5 Managing DNAT Rules](#)

## 3.5.2 Modifying a DNAT Rule

### Scenarios

After a DNAT rule is added, you can modify parameters in the DNAT rule as required.

Note that modifying a DNAT rule may interrupt your services.

### Prerequisites

A DNAT rule has been added.

### Procedure

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click the name of the private NAT gateway.

3. On the private NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, locate the DNAT rule you want to modify and click **Modify** in the **Operation** column.
5. In the displayed dialog box, modify parameters as needed.  
On the local network, the port type, protocol, instance type, and internal port can be modified.  
On the transit network, the transit IP address, transit IP address port, and description can be modified.
6. Click **OK**.

### 3.5.3 Deleting a DNAT Rule

#### Scenarios

You can delete DNAT rules that are no longer needed.

#### Prerequisites

A DNAT rule has been added.

#### Procedure

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, click the name of the private NAT gateway.
3. On the private NAT gateway details page, click the **DNAT Rules** tab.
4. In the DNAT rule list, locate the DNAT rule you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

## 3.6 Managing Transit IP Addresses

### 3.6.1 Assigning a Transit IP Address

#### Scenarios

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

A transit IP address can be mapped to multiple backend servers through different ports.

#### Procedure

1. Go to the [private NAT gateway list](#) page.
2. On the **Private NAT Gateways** page, choose **Transit IP Addresses > Assign Transit IP Address**.

**Figure 3-5** Assigning a transit IP address

3. Configure required parameters. For details, see [Table 3-6](#).

**Table 3-6** Parameter descriptions of a transit IP address

Parameter	Description
Transit VPC	VPC to which the transit IP address is located.
Transit Subnets	A transit subnet is a transit network where transit IP addresses are assigned. The subnet must have at least one available IP address.
Transit IP Address	How the transit IP address will be assigned. There are two options: <b>Automatic:</b> The system automatically assigns a transit IP address. <b>Manual:</b> You need to manually assign a transit IP address.
IP Address	This parameter is only available when you set <b>Transit IP Address</b> to <b>Manual</b> . Click <b>View In-Use IP Address</b> to view in-use IP addresses in the selected subnet.
Enterprise Project	The enterprise project to which the transit IP address belongs.
Tag	The transit IP address tag, which consists of a key and value pair. You can add up to 20 tags to each transit IP address.

4. Click **OK**.

## 3.6.2 Viewing a Transit IP Address

### Scenarios

You can view the details about a transit IP address.

### Procedure

1. Go to the [private NAT gateway list](#) page.
2. Click the **Transit IP Addresses** tab and then click the transit IP address.
3. On the page displayed, view the details of the transit IP address.  
You can view the transit VPC, transit subnet, and private NAT gateway associated with the transit IP address.

## 3.6.3 Releasing a Transit IP Address

### Scenarios

You can release a transit IP address that is no longer needed.

### Procedure

1. Go to the [private NAT gateway list](#) page.
2. In the **Transit IP Addresses** tab, locate the transit IP address you want to release and click **Release** in the **Operation** column.
3. Click **OK**.

#### 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, disassociate all rules associated from it first.

# 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 NAT gateway on the NAT gateway details page. A maximum of 20 tags can be added 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.

A tag consists of a key and value pair. [Table 4-1](#) lists the tag key and value requirements.

**Table 4-1** Tag key and value requirements

Parameter	Requirement
Key	<ul style="list-style-type: none"> <li>• Cannot be left blank.</li> <li>• Must be unique for each NAT gateway.</li> <li>• Can contain a maximum of 36 characters.</li> <li>• Cannot contain equal signs (=), asterisks (*), left angle brackets (&lt;), right angle brackets (&gt;), backslashes (\), commas (,), vertical bars ( ), and slashes (/), and cannot start or end with spaces.</li> </ul>
Value	<ul style="list-style-type: none"> <li>• Can contain a maximum of 43 characters.</li> <li>• Cannot contain equal signs (=), asterisks (*), left angle brackets (&lt;), right angle brackets (&gt;), backslashes (\), commas (,), vertical bars ( ), and slashes (/), and cannot start or end with spaces.</li> </ul>

## Managing NAT Gateway Tags

You can manage tags for NAT gateways in either of the following ways:

- Add tags when you create a NAT gateway.  
For detailed operations, see [2.2 Buying a Public NAT Gateway](#) and [3.2 Buying a Private NAT Gateway](#).
- Modify tags for an existing NAT gateway.
  - a. Go to the [NAT gateway list page](#).
  - b. In the public or private NAT gateway list, click the target NAT gateway.
  - c. Under **Tags**, click **Edit Tag**.
  - d. The **Edit Tag** dialog box is displayed.
    - i. Adding a tag: On the **Edit Tag** page, click **Add** and enter a tag key and tag value.
    - ii. Modifying a tag: On the **Edit Tag** page, locate the target tag and enter a new value.
  - e. Click **OK**.

 **NOTE**

- A maximum of 20 tags can be added to a NAT gateway.
- Each tag is a key-value pair, and the tag key is unique.

You can manage tags for transit IP addresses in either of the following ways:

- Add tags when you assign a transit IP address.  
For details, see [3.6.1 Assigning a Transit IP Address](#).
- Modify tags for an existing transit IP address.
  - a. Go to the [transit IP address list](#) page.
  - b. In the transit IP address list of the private NAT gateway, click the target transit IP address.
  - c. Click **Edit Tag**.
  - d. The **Edit Tag** dialog box is displayed.
    - i. Adding a tag: On the **Edit Tag** page, click **Add** and enter a tag key and tag value.
    - ii. Modifying a tag: On the **Edit Tag** page, locate the target tag and enter a new value.
  - e. Click **OK**.

 **NOTE**

- A maximum of 20 tags can be added to a transit IP address.
- Each tag is a key-value pair, and the tag key is unique.


# 5 Managing Quotas

## What Is the Quota?

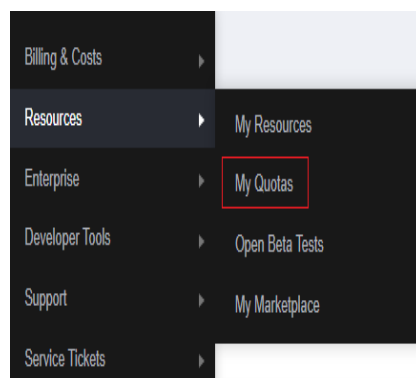
Quotas are enforced for service resources on the platform to prevent unforeseen spikes in resource usage. Quotas can limit the number or capacity of resources available to users. For example, the quota can limit the maximum number of EIPs that can be associated with an SNAT rule. You can apply for increasing quotas if necessary.

This section describes how to view the used NAT Gateway quota and the total NAT Gateway quota in a specified region.

## How Do I View My Quotas?

1. Log in to the [management console](#).
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Quotas** page is displayed.

**Figure 5-1** My Quotas

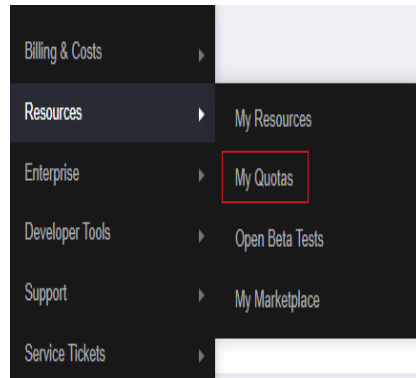


4. View the used and total quota of each type of resources on the displayed page.  
If a quota cannot meet service requirements, apply for a higher quota.

## How Do I Apply for a Higher Quota?

1. Log in to the [management console](#).
2. In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Quotas** page is displayed.

**Figure 5-2 My Quotas**



3. Click **Increase Quota** in the upper right corner of the page.

**Figure 5-3 Increasing quota**

Service	Resource Type	Used Quota	Total Quota
Auto Scaling	AS group	0	
	AS configuration	0	
Image Management Service	Image	0	
Cloud Container Engine	Cluster	0	
FunctionGraph	Function	0	
	Code storage(MB)	0	
Elastic Volume Service	Disk	3	
	Disk capacity(GB)	120	
Storage Disaster Recovery Service	Snapshots	4	
	Protection group	0	
Cloud Server Backup Service	Replication pair	0	
	Backup Capacity(GB)	0	
Scalable File Service	Backup	0	
	File system	0	
CDN	File system capacity(GB)	0	
	Domain name	0	
	File URL refreshing	0	
	Director URL refreshing	0	
	URL prewarming	0	

4. On the **Create Service Ticket** page, configure parameters as required.  
In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

# 6 Monitoring

---

[6.1 Monitoring NAT Gateway Resources](#)

[6.2 NAT Gateway Monitoring Metrics](#)

## 6.1 Monitoring NAT Gateway Resources

### Scenarios

Cloud Eye is a multi-dimensional resource monitoring service. You can use Cloud Eye to monitor NAT Gateway resources in real time, set alarm rules, identify resource exceptions, and quickly respond to resource changes.

Cloud Eye is enabled automatically after a resource is created. For more information about Cloud Eye, see [What Is Cloud Eye?](#)

### Setting an Alarm Rule

You can configure alarm rules on the Cloud Eye console to send you notifications in case of exceptions.

For details about how to set alarm rules, see [Creating an Alarm Rule](#).

### Viewing Monitoring Metrics

Cloud Eye monitors [NAT Gateway metrics](#) in real time. You can view monitoring details of each metric on the Cloud Eye console.

For details about how to view NAT Gateway monitoring metrics on the Cloud Eye console, see [Querying Metrics of a Cloud Service](#).

## 6.2 NAT Gateway Monitoring 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 6-1** Public NAT gateway metrics

Metric ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway	≥ 0	Count	N/A	Public NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Total bandwidth sent out through the public NAT gateway from the public network	≥ 0	bit/s	1024 (IEC)	Public NAT gateway	1 minute
outbound_bandwidth	Outbound Bandwidth	Total bandwidth sent out through the public NAT gateway from the VPC	≥ 0	bit/s	1024 (IEC)	Public NAT gateway	1 minute
inbound_pps	Inbound PPS	Packets received by the public NAT gateway from the public network per second	≥ 0	Count	N/A	Public NAT gateway	1 minute
outbound_pps	Outbound PPS	Packets received by the public NAT gateway from the VPC per second	≥ 0	Count	N/A	Public NAT gateway	1 minute
inbound_traffic	Inbound Traffic	Traffic sent through the public NAT gateway from the public network	≥ 0	Byte	1024 (IEC)	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
outbound_traffic	Outbound Traffic	Traffic sent through the public NAT gateway from the VPC	≥ 0	Byte	1024 (IEC)	Public NAT gateway	1 minute
snat_connection_ratio	SNAT Connection Usage Rate	Usage rate of SNAT connections The maximum number of connections is the number of connections allowed by NAT gateway specifications. For details, see <a href="#">NAT Gateway Specifications</a> .	≥ 0	%	N/A	Public NAT gateway	1 minute
inbound_bandwidth_ratio	Inbound Bandwidth Usage Rate	Ratio of the bandwidth used by the public NAT gateway to route traffic from the public network 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 × 100%. <b>NOTE</b> This metric is used to monitor the performance of public NAT gateways instead of the EIP bandwidth.	≥ 0	%	N/A	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
outbound_bandwidth_ratio	Outbound Bandwidth Usage Rate	<p>Ratio of the bandwidth used by the public NAT gateway to route traffic from the VPC</p> <p>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 × 100%.</p> <p><b>NOTE</b> This metric is used to monitor the performance of public NAT gateways instead of the EIP bandwidth.</p>	≥ 0	%	N/A	Public NAT gateway	1 minute
total_inbound_udp_bandwidth	Total Inbound Bandwidth (UDP)	Total bandwidth sent out through the public NAT gateway over UDP from the public network	≥ 0	bit/s	1024 (IEC)	Public NAT gateway	1 minute
total_outbound_udp_bandwidth	Total Outbound Bandwidth (UDP)	Total bandwidth sent out through the public NAT gateway over UDP from the VPC	≥ 0	bit/s	1024 (IEC)	Public NAT gateway	1 minute
total_inbound_tcp_bandwidth	Total Inbound Bandwidth (TCP)	Total bandwidth sent out through the public NAT gateway over TCP from the public network	≥ 0	bit/s	1024 (IEC)	Public NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
total_outbound_tcp_bandwidth	Total Outbound Bandwidth (TCP)	Total bandwidth sent out through the public NAT gateway over TCP from the VPC	$\geq 0$	bit/s	1024 (IEC)	Public NAT gateway	1 minute
packets_drop_count_snat_connection_beyond	Packets Dropped (Excessive SNAT Connections)	Number of packets dropped by the public NAT gateway due to excessive SNAT connections	$\geq 0$	Count	N/A	Public NAT gateway	1 minute
packets_drop_count_pps_beyond	Packets Dropped (Excessive PPS)	Number of packets dropped by the public NAT gateway due to excessive PPS	$\geq 0$	Count	N/A	Public NAT gateway	1 minute
packets_drop_count_eip_port_alloc_beyond	Packets Dropped (When All EIP Ports Allocated)	Number of packets dropped by the public NAT gateway when all EIP ports have been allocated	$\geq 0$	Count	N/A	Public NAT gateway	1 minute

**Table 6-2** Private NAT gateway metrics

Metric ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
snat_connection	SNAT Connections	Number of SNAT connections of the NAT gateway	$\geq 0$	Count	N/A	Private NAT gateway	1 minute
inbound_bandwidth	Inbound Bandwidth	Bandwidth used by the private NAT gateway to receive traffic from the VPC where the transit IP address is assigned	$\geq 0$	bit/s	1024 (IEC)	Private NAT gateway	1 minute
outbound_bandwidth	Outbound Bandwidth	Bandwidth used by the private NAT gateway to receive traffic from the VPC where this gateway is created	$\geq 0$	bit/s	1024 (IEC)	Private NAT gateway	1 minute
inbound_pps	Inbound PPS	Packets received by the private NAT gateway per second from the VPC where the transit IP address is assigned	$\geq 0$	Count	N/A	Private NAT gateway	1 minute
outbound_pps	Outbound PPS	Packets received by the private NAT gateway per second from the VPC where this gateway is created	$\geq 0$	Count	N/A	Private NAT gateway	1 minute
inbound_traffic	Inbound Traffic	Traffic received by the private NAT gateway from the VPC where the transit IP address is assigned	$\geq 0$	Byte	1024 (IEC)	Private NAT gateway	1 minute

Metric ID	Name	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Period (Raw Data)
outbound_traffic	Outbound Traffic	Traffic received by the private NAT gateway from the VPC where this gateway is created	≥ 0	Byte	1024 (IEC)	Private NAT gateway	1 minute
packets_dropped_count_snat_connection_beyond	Packets Dropped (Excessive SNAT Connections)	Number of packets dropped by the public NAT gateway due to excessive SNAT connections	≥ 0	Count	N/A	Private NAT gateway	1 minute
packets_dropped_count_pps_beyond	Packets Dropped (Excessive PPS)	Number of packets dropped by the public NAT gateway due to excessive PPS	≥ 0	Count	N/A	Private NAT gateway	1 minute
packets_dropped_count_eip_port_alloc_beyond	Packets Dropped (When All EIP Ports Allocated)	Number of packets dropped by the public NAT gateway when all EIP ports have been allocated	≥ 0	Count	N/A	Private NAT gateway	1 minute

## Dimensions

Key	Value
nat_gateway_id	Public NAT gateway
vpc_nat_gateway_id	Private NAT gateway

# 7 Auditing

## [7.1 Key Operations Recorded by CTS](#)

### [7.2 Viewing Traces](#)

## 7.1 Key Operations Recorded by CTS

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

**Table 7-1** lists public NAT gateway operations that can be recorded by CTS.

**Table 7-2** lists private NAT gateway operations that can be recorded by CTS.

**Table 7-1** Public NAT gateway operations

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

Operation	Resource Type	Trace
Querying a public NAT gateway	natgateways	showNatGateway
Querying public NAT gateways	natgateways	showSnatRule
Querying the details of a SNAT rule on a public NAT gateway	snatrules	listSnatRule
Querying SNAT rules on a public NAT gateway	snatrules	listSnatRule
Querying the details of a DNAT rule on a public NAT gateway	dnatrules	showDnatRule
Querying DNAT rules on a public NAT gateway	dnatrules	listDnatRule
Adding, modifying, or deleting NAT gateway tags	tag	batchUpdateTags

**Table 7-2** Private NAT gateway operations

Operation	Resource Type	Trace
Creating a private NAT gateway	privateNat	createPrivateNat
Modifying a private NAT gateway	privateNat	updatePrivateNat
Deleting a private NAT gateway	privateNat	deletePrivateNat
Creating a DNAT rule	privateDnatRule	createPrivateDnatRule
Modifying a DNAT rule	privateDnatRule	updatePrivateDnatRule
Deleting a DNAT rule	privateDnatRule	deletePrivateDnatRule
Creating an SNAT rule	privateSnatRule	createPrivateSnatRule
Modifying an SNAT rule	privateSnatRule	updatePrivateSnatRule
Deleting an SNAT rule	privateSnatRule	deletePrivateSnatRule



Operation	Resource Type	Trace
Assigning a transit IP address	transitIp	createTransitIp
Releasing a transit IP address	transitIp	deleteTransitIp
Querying a private NAT gateway	privateNat	showPrivateNat
Querying private NAT gateways	privateNat	listPrivateNat
Querying the details of a SNAT rule on a private NAT gateway	privateSnatRule	showPrivateSnatRule
Querying SNAT rules on a private NAT gateway	privateSnatRule	listPrivateSnatRule
Querying the details of a DNAT rule on a private NAT gateway	privateDnatRule	showPrivateDnatRule
Querying DNAT rules on a private NAT gateway	privateDnatRule	listPrivateDnatRule
Querying a transit IP address	transitIp	showTransitIp
Querying transit IP addresses	transitIp	listTransitIp
Adding, modifying, or deleting NAT gateway tags	privateNat	batchCreateDeletePrivateNat-Tag
Querying a private NAT gateway tag	privateNat	showPrivateNatTag
Querying private NAT gateway tags	privateNat	listPrivateNatTag
Adding, modifying, or deleting transit IP address tags	transitIp	batchCreateDeleteTransitIpTag
Querying a transit IP address tag	transitIp	showTransitIpTag
Querying tags of a transit IP address	transitIp	listTransitIpTag

## 7.2 Viewing Traces

### Scenarios

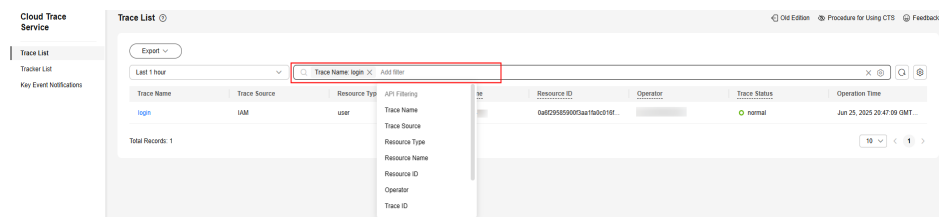
CTS records the operations performed on NAT Gateway and allows you to view the operation records of the last seven days on the CTS console. This topic describes how to query these records on the CTS console.

### 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. In the upper left corner of the page, click  to go to the service list. Under **Management & Governance**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. In the trace list, specify filters as needed.

For details about the parameters for filtering traces, see [Viewing Traces](#) in the *Cloud Trace Service User Guide*.

**Figure 7-1** Advanced search



6. Locate the trace and click its name and check the trace details in the dialog box displayed on the right.

**Figure 7-2** Trace list

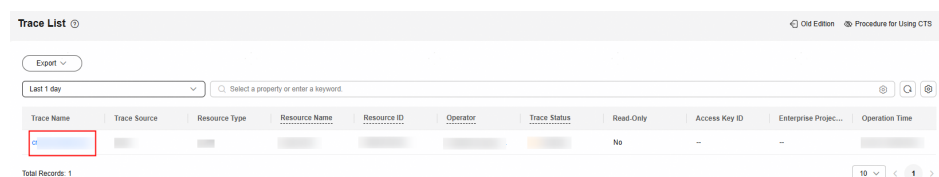


Figure 7-3 Trace overview

The screenshot displays the 'Trace Overview' interface. At the top right is a close button (X). Below the title is a 'Basic Information' section with a link 'Learn about trace structure'. This section contains two columns of fields: Trace ID, Occurred, Operator, Return Code, Trace Source, Resource Type, Resource Name, and Source IP Address. Below this is a dark-themed code editor showing a JSON trace log. The log includes fields like 'api\_version', 'code' (400), 'domain\_id', 'event\_type', 'message', 'operation\_id', 'project\_id', 'read\_only', 'resource\_acc', 'resource\_id', 'resource\_name', 'resource\_type', 'service\_type', 'source\_ip', 'trace\_id', 'trace\_name', 'trace\_rating', 'trace\_type', 'tracker\_name', 'user' (with sub-fields 'domain', 'xdomain', 'name', 'id', 'xdomain'), and 'request'.

7. For more information about CTS, see the [Cloud Trace Service User Guide](#).