Alibaba Cloud NAT Gateway

User Guide

Issue: 20190516

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Specifications of NAT Gateway

You can select different specifications for NAT Gateway to adjust the performance metrics (maximum connections and the number of new connections per second). However, data throughput is not affected.

The following table lists the available specifications for NAT Gateway.

Specification	Maximum number of SNAT connections	Number of new SNAT connections established per second
Small	10,000	1,000
Medium	50,000	5,000
Large	200,000	10,000
Super Large-1	1,000,000	30,000

Note the following when selecting a specification:

- NAT Gateway specifications impact SNAT performance only (they do not affect DNAT performance).
- There is no correlation between a specification and the number of IPs.
- CloudMonitor only provides monitoring data on the maximum number of connections. It does not provide monitoring data on CPS.
- The timeout period of an SNAT connection is 900 seconds.
- To avoid SNAT connection timeout caused by network congestion and public network jitter, make sure that your service application has implemented automatic reconnection to provide higher availability.
- Currently, NAT Gateway does not support packet fragmentation.
- For the same destination public IP address and port, the number of EIPs that are associated with a NAT Gateway affects the maximum number of connections that the NAT Gateway can handle. If the NAT Gateway is associated with only one EIP , the maximum number of connections is 50,000. If multiple EIPs are associated, this number is 50,000 multiplied by the number of EIPs..
- ECS instances in a VPC that are not associated with any public IP addresses can access the Internet through a NAT Gateway. If the bandwidth at which the ECS instances access the same public IP address and port is greater than 2

Gbit/s, packets may be discarded due to limited ports. To resolve this issue, we recommend that you associate four to eight EIPs with the NAT Gateway and *create a SNAT pool*.

2 Manage a NAT Gateway

This topic describes how to create, modify, and delete a NAT Gateway.

Create a NAT Gateway instance

To create a NAT Gateway instance, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Click Create NAT Gateway.
4. Configure the NAT Gateway according to the following information and complete the payment.

Configuration	Description
Region	Select the region to which the NAT Gateway will be located. Make sure the regions of the NAT Gateway and VPC are the same.
VPC ID	Select the VPC for which the NAT Gateway is created. After the gateway is created, you cannot change the VPC. If you cannot find the target VPC in the VPC list, troubleshoot as follows: · Check whether the VPC already has a NAT Gateway configured. A VPC can be configured with only one NAT Gateway. · Check whether a custom route entry, whose destination CIDR block is 0.0.0.0/0, already exists in the VPC. If so, delete this custom route entry.
Specifications	Select a specification for the NAT Gateway. The specification affects the maximum number of connections and the number of new connections allowed per second for the SNAT proxy service, but does not affect data throughput. Note: The specification does not limit the number of connections and throughput of the DNAT function. For more information, see *Specifications of NAT Gateway*.
Billing Cycle	Select a billing cycle for the NAT Gateway.

Change the specification of a NAT Gateway

You can change the specification of a NAT Gateway according to your business needs . The specification of the NAT Gateway only affects the performance of SNAT; it does not affect on the DNAT performance.

To change the specification for a NAT Gateway, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. Click the instance ID of the target NAT Gateway.
5. On the NAT Gateway Details page, click Change Specification.
6. In the Configuration upgrade area, select a new specification and then click Activate.

Edit a NAT Gateway

To edit the name or description of a NAT Gateway, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. Click the ID of the target NAT Gateway.
5. On the NAT Gateway Details page, click Edit next to the name and description. Enter a name or description and then click OK.

Delete a NAT Gateway

To delete a NAT Gateway, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the target NAT Gateway.
4. Find the target NAT Gateway, and then click Delete. In the displayed dialog box, click OK.

 **Note:**

You can also click Delete (Delete NAT Gateway and resources) to forcibly delete the NAT Gateway. After the NAT Gateway is deleted, the EIP is disassociated automatically.

3 Manage a DNAT table

You can use the DNAT function to map a public IP to a private IP of an ECS instance in the VPC network. Then, the ECS instance with the specified public IP can provide public services.

DNAT entries

The DNAT function in the NAT gateway is abstracted as a DNAT table. You can create a DNAT entry to use the DNAT function.

A DNAT entry consists of public IP, public port, private IP, private port, and protocol. The public IP is the bound EIP whereas the private IP is the private IP address of the ECS instance. After configuring a DNAT entry, the data packet received from the specified public IP will be forwarded to the ECS instance according to the mapping rule.

> Note:
> If your account has purchased a bandwidth package before January 26, 2018, the public IP is the IP of the bandwidth package.

Port mapping and IP mapping

The DNAT function includes port mapping and IP mapping:

- Port mapping

  With port mapping, the NAT Gateway will forward requests from specified protocol and port to the selected ECS instance of the specified port in the VPC. Such as the Entry 1 and Entry 2 in the following table.

- IP mapping

  With IP mapping, the NAT Gateway will forward requests from the specified IP to the selected ECS instances in the VPC, like binding an EIP to the ECS instance. Any request to access the public IP is forwarded to the target ECS instance. Such as the Entry 3 in the following table.

DNAT entry	Public IP	Public port	Private IP	Private port	Protocol
Entry 1	139.224.xx.xx	80	192.168.x.x	80	TCP

DNAT entry	Public IP	Public port	Private IP	Private port	Protocol
Entry 2	139.224.xx.xx	8080	192.168.x.x	8000	UDP
Entry 3	139.224.xx.xx	Any	192.168.x.x	Any	Any

Add a DNAT entry

To add a DNAT entry, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. Click the ID of the target NAT Gateway.
5. In the left-side navigation pane, click DNAT Table, and then click Create DNAT Entry.
6. Configure the DNAT entry according to the following information.

Configuration	Description
Public IP	Select a public IP. Note: The IP that is already being used in an SNAT entry cannot be selected.
Private IP	Select the private IP of the ECS instance to access the Internet. You can specify the private IP in the following ways : · Manually Input: Enter the private IP that you want to map. It must be within the private IP range of the VPC. · Auto Fill: Select an ECS instance in the VPC from the list. The private IP of the selected ECS instance is automatically entered in the field.

Configuration	Description
Port Settings	DNAT supports IP mapping and port mapping. Select a mapping method: · All Ports: Select this option to configure IP mapping. Using this method, the ECS instance with the specified private IP can receive any Internet requests using any protocol on any port. This is the same as binding an EIP to the ECS instance. · Specific Port: Select this option to configure port mapping. Using this method, NAT Gateway forwards the request from the specified protocol and port to the target ECs instance on the specified port. You must specify the public port, private port, and IP protocol when the port mapping is selected.

Edit a DNAT entry

To edit a DNAT entry, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. Click the Configure DNAT option of the target NAT Gateway.
5. Click Edit to edit the target DNAT entry.

Delete a DNAT entry

To delete a DNAT entry, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the target NAT Gateway.
4. Click the Configure DNAT option of the target NAT Gateway.
5. Click Remove, and then click OK in the displayed dialog box.

4 Manage an SNAT table

The SNAT function provides an Internet proxy service for ECS instances located in a VPC that do not have public IP addresses to be permitted access to the Internet.

SNAT entries

The SNAT function in the NAT Gateway is abstracted as an SNAT table. You can create an SNAT entry in the SNAT table to use the SNAT function.

Each SNAT entry consists of a VSwitch and a public IP address. The VSwitch is where the ECS instance to use the SNAT function is located and the public IP address is the Elastic IP Address (EIP) associated with the NAT Gateway, as shown in the following table.

 Note:
If you purchased a bandwidth package before January 26, 2018, the public IP address is the IP address of the bandwidth package.

VSwitch	Public IP address
vsw-184ipsxxx	139.224.xx.xx
vsw-11qht5xxx	139.224.xx.xx

After you configure an SNAT entry, when an ESC instance in the specified VSwitch initiates an Internet access request, NAT Gateway will provide it with the Internet proxy service so that the ECS instance can use the specified public IP address to access the Internet. By default, all the ECS instances belonging to the VSwitch can use the specified public IP address to access the Internet.

 Note:
If an ECS instance is already configured with a public IP address (such as an EIP), the system will use the pre-configured public IP address to access the Internet and will not activate the SNAT function.

Add an SNAT entry

To add an SNAT entry, follow these steps:

1. Log on to the *VPC console*.

2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the target NAT Gateway.
4. Find the target NAT Gateway and click its NAT Gateway ID.
5. In the left-side navigation pane, click SNAT Table, and then click Create SNAT Entry.
6. Configure the SNAT entry according to the following information.

Configuration	Description
VSwitch Granularity	
VSwitch	Select the VSwitch where the ECS instances that require the Internet access are located. All ECS instances that belong to the specified VSwitch can use the specified public IP address to access the Internet.  Note: If an ECS instance is already configured with a public IP address (such as an EIP), the pre-configured public IP address is used to access the Internet instead of using the SNAT proxy service.
VSwitch CIDR Block	Displays the CIDR block of the selected VSwitch.
Public IP	Select the public IP address that is used to access the Internet.  Note: The IP that is already being used in a DNAT entry cannot be selected.
Entry Name	Enter a name for the SNAT entry to be created. The name must be 2 to 128 characters in length and can contain letters, numbers, Chinese characters, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
ECS Granularity	

Configuration	Description
Available ECS Instances	Select an ECS instance in the corresponding VPC that needs to access the Internet. The selected ECS instance will access the Internet by using the specified public IP address. Make sure that: · The ECS instance is running. · The ECS instance is not associated with any dedicated public IP addresses or EIPs.
ECS CIDR Block	Displays the CIDR block of the selected ECS instance.
Public IP	Select a public IP address that the ECS instance can use to access the Internet. Note: The public IP address that is already used for a DNAT entry cannot be used for an SNAT entry.

Edit an SNAT entry

To edit an SNAT entry, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. Find the target NAT Gateway and click Configure SNAT in the Actions column.
5. Click Edit on the right of the target SNAT entry to edit the SNAT configurations.

Delete an SNAT entry

To delete an SNAT entry, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the NAT Gateway.
4. Find the target NAT Gateway and click Configure SNAT in the Actions column.
5. Click Remove on the right of the target SNAT entry, and then click OK.

5 Associate and disassociate EIPs

After you create a NAT Gateway, you must configure public IP addresses for the NAT Gateway. To do so, you can associate one or more Elastic IP Addresses (EIPs) with the NAT Gateway.

> Note:
>
> If you purchased a NAT bandwidth package for your account before January 26, 2018 , you cannot associate EIPs with the NAT Gateway. If you want to associate EIPs with the NAT Gateway, open a ticket.

Associate an EIP with a NAT Gateway

> Note:
>
> Make sure that you have created a NAT Gateway and an EIP.

To associate an EIP with a NAT Gateway, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the target NAT Gateway.
4. Find the target NAT Gateway and choose More > Bind Elastic IP Address in the Actions column.
5. In the displayed dialog box, complete the following configurations:
   a. Public IP: Select the EIP to be associated with the NAT Gateway.
   b. VSwitches (Optional): If you select a VSwitch, the system automatically adds an SNAT rule so that cloud products under the VSwitch can access the Internet through the selected EIP.
6. To associate more EIPs with the NAT Gateway, repeat the previous steps.

Disassociate an EIP from a NAT Gateway

> Note:
>
> Make sure the EIP to be disassociated is not being used by any SNAT entries or DNAT entries.

To disassociate an EIP, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click NAT Gateways.
3. Select the region of the target NAT Gateway.
4. Find the target NAT Gateway and choose More > Unbind Elastic IP Address.
5. In the displayed dialog box, select the target EIP and click OK.

6 Anti-DDoS

Alibaba Cloud provides up to 5 Gbps basic anti-DDoS protection for NAT Gateway. As shown in the following figure, all traffic from the Internet must first go through Alibaba Cloud Security before arriving at NAT Gateway. Anti-DDoS Basic scrubs and filters common DDoS attacks and protects your services against attacks such as SYN flood, UDP flood, ACK flood, ICMP flood, and DNS flood.

Anti-DDoS Basic sets the scrubbing threshold and blackholing threshold according to the EIP bandwidth of NAT Gateway. When the inbound traffic reaches the threshold, scrubbing or blackholing is triggered:

- Scrubbing: When the attack traffic from the Internet exceeds the scrubbing threshold or matches certain attack traffic model, Alibaba Cloud Security starts scrubbing the attack traffic. The scrubbing includes packet filtration, traffic speed limitation, packet speed limitation and more.
- Blackholing: When the attack traffic from the Internet exceeds the blackholing threshold, blackholing is triggered and all inbound traffic is dropped.

The scrubbing thresholds of NAT Gateway are calculated as follows. If the EIP bandwidth is 1,000 Mbps, the maximum traffic scrubbing threshold (bits/s) is 1,000 Mbps, the maximum traffic scrubbing threshold (packets/s) is 150,000 and the default blackholing threshold is 2 Gbps.

EIP bandwidth	Maximum traffic scrubbing threshold (bits/s)	Maximum traffic scrubbing threshold (packets/s)	Default blackholing threshold
Less than or equal to 800 Mbps	800 Mbps	120,000	1.5 Gbps
More than 800 Mbps	Configured bandwidth	Configured bandwidth × 150	Configured bandwidth × 2

7 Manage quotas

You can query the number of remaining resources in your quota through the VPC console. If the remaining quota number is insufficient for your requirements, you can open a ticket to apply for an increase to your quota.

Procedure

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click Quota Management.
3. On the Quota Management page, click the NAT Gateways tab to view the quota usage of VPCs under your account.
4. To increase your resource quota, click Apply in the Actions column. Then, enter the following information.
   - Quantity for Application: the number of resources you require. You must enter a number that is larger than the current quota. For more information about the resource limits of NAT Gateway, see *Limits*.
   - Reason for Application: your reason for applying for an increase to your quota. We recommend that you include details about your specific scenario.
   - Mobile/Landline Phone Number: the mobile or landline phone number of the person to contact.
   - Email: the email address of the person to contact.
5. Click OK.

   The system then determines whether the quota application is reasonable.

   - If the system determines the request is unreasonable, the application enters the Rejected state.
   - If the application is reasonable, the application status enters the Approved state and the quota is automatically upgraded to the specified quota number.

   To view the history of quota applications, click Application History in the Application History column.

8 View monitoring data

Because NAT Gateway interoperates with Alibaba CloudMonitor, you can view the monitoring data of NAT Gateway, such as the number of connections, and the number of discarded connections due to the capacity or speed limit being reached.

Procedure

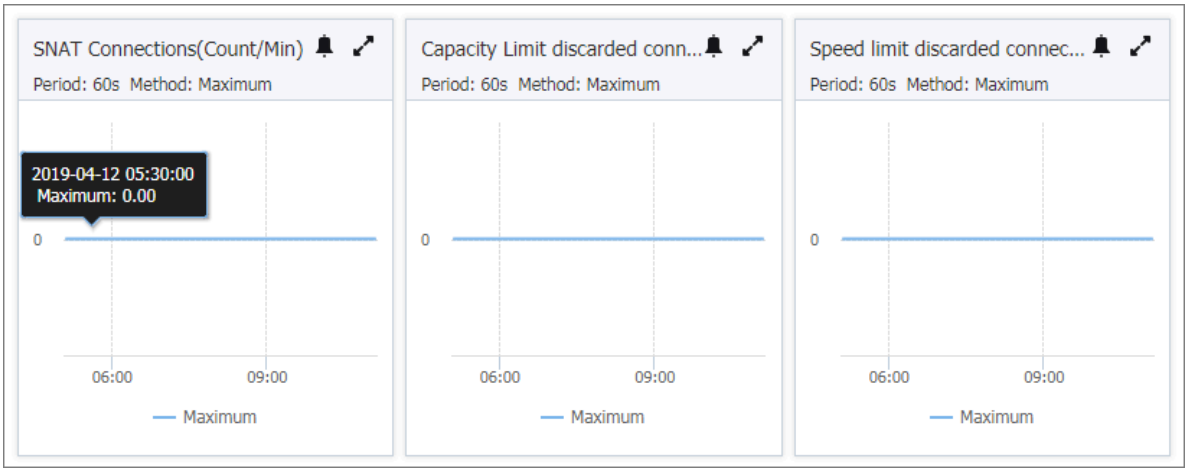
1. Log on to the *VPC console*.
2. Click NAT Gateways and then select the region of the target NAT Gateway.
3. Click the monitoring icon  in the SNAT Connections column of the target instance to view the monitoring data.

   Monitoring metrics of a NAT Gateway are shown in the following table:

Item	Description	Dimension	Unit	Minimum monitoring granularity
SNAT connections	The SNAT connections of a NAT Gateway instance.	Instance	Count/Min	30s

Item	Description	Dimension	Unit	Minimum monitoring granularity
Capacity limit discarded connections	The maximum number of SNAT connections vary according to the NAT Gateway specification. Capacity limit discarded connections indicate the SNAT connections that are dropped when the number of connections to the instance exceeds the maximum number of SNAT connections corresponding to the specification of the instance. Note: This metric is an accumulated value and will not be reset. · If the number of capacity limit discarded connections increase continuously during a certain period of time, we recommend that you upgrade the specification of NAT Gateway. · If a horizontal line is displayed during a certain period of time, it indicates that no packets were dropped during this time period.	Instance	Count/Min	30s

Item	Description	Dimension	Unit	Minimum monitoring granularity
Speed limit discarded connections	The maximum number of SNAT connections per second vary according to the NAT Gateway specification. Speed limit discarded connections indicate the number of SNAT connections that are dropped when the number of SNAT connections to the instance per second exceeds the maximum number of SNAT connections per second corresponding to the specification of the instance.  Note: This metric is an accumulated value and will not be reset. · If the number of speed limit discarded connections increase continuously during a certain period of time, we recommend that you upgrade the specification of the NAT Gateway. · If a horizontal line is displayed during a certain period of time, it indicates that no packets were dropped during this time period.	Instance	Count/Min	30s


SNAT Connections(Count/Min)
Period: 60s Method: Maximum
2019-04-12 05:30:00
Maximum: 0.00
0
06:00
09:00
Maximum
Capacity Limit discarded conn...
Period: 60s Method: Maximum
0
06:00
09:00
Maximum
Speed limit discarded connec...
Period: 60s Method: Maximum
0
06:00
09:00
Maximum