ALIBABA CLOUD

Alibaba Cloud

NAT Gateway
User Guide

Document Version:

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Types of NAT gateway

Network Address Translation (NAT) gateways can be divided into the following types: Small, Middle, Large, and Super Large-1. The type of NAT gateway that you choose determines the maximum number of Source Network Address Translation (SNAT) connections and the number of new SNAT connections per second. However, it does not affect the performance of Destination Network Address Translation (DNAT).

Comparison

The following table lists the types of NAT gateway.

Type	Maximum number of SNAT connections	Number of new SNAT connections per second
Small	10,000	1,000
Middle	50,000	5,000
Large	200,000	10,000
Super Large-1	1,000,000	50,000

Limits

When you select a type of NAT gateway, note the following limits:

- The bandwidth and the number of IP addresses in a NAT service plan are not restricted by the type of NAT gateway that you choose.
- CloudMonitor monitors only the maximum number of SNAT connections for NAT gateways. It does not monitor the number of new SNAT connections per second.
- The timeout of SNAT connections in a NAT gateway is 900 seconds.
- To avoid the timeout of SNAT connections caused by network congestion and Internet instability, make sure that your applications support automatic reconnection, which ensures higher availability.
- NAT gateways do not support packet fragmentation.
- For the same destination public IP address and port, the number of Elastic IP addresses configured for a NAT gateway determines the maximum number of concurrent connections. If an individual Elastic IP address is bound to the NAT gateway, the maximum number of connections is 55,000. If N Elastic IP addresses are bound to the NAT gateway, the maximum number of connections is increased to N × 55,000.
- Assume that you have multiple ECS instances deployed in a VPC network and the ECS instances are not assigned public IP addresses. The ECS instances access the same destination IP address and port on the Internet through a NAT gateway at a bandwidth higher than 2 Gbit/s. To avoid packet loss caused by the upper limit of ports for a single public IP address, we recommend that you bind 4 to 8 public IP addresses to the NAT gateway and create a SNAT pool.

2.Manage a NAT Gateway

2.1. Create a NAT Gateway

This topic describes how to create a NAT Gateway. You must create a NAT Gateway before configuring SNAT and DNAT entries.

Prerequisites

A VPC and a VSwitch are created. For more information, see Create a VPC network.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. On the **NAT Gateways** page, click **Create NAT Gateway**.
4. On the displayed purchase page, configure the NAT Gateway and complete the payment. The following table describes the parameters.

Configuration	Description
Region	Select the region where the target VPC (to which the NAT Gateway belongs) is located.
VPC ID	Select the VPC for which you want to create a NAT Gateway. After the NAT Gateway is created, you cannot change the VPC. Note If you cannot find the target VPC in the VPC list, troubleshoot as follows: ○ Check whether a NAT Gateway is already configured for the VPC. A VPC can be configured with only one NAT Gateway. ○ Check whether there is a custom route entry whose destination CIDR block is 0.0.0.0/0 in the VPC. If so, delete this custom route entry.
Specification	Select a specification for the NAT Gateway. Different specifications correspond to different Max Connections and Connections Per Second (CPS) of the SNAT function. However, the data throughput is not affected. Note The specification does not limit the number of connections and throughput of the DNAT function. For more information, see Types of NAT gateway.
Billing cycle	Select a billing cycle for the NAT Gateway.

2.2. Edit a NAT Gateway

This topic describes how to modify the name and description of a NAT Gateway.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, find the target NAT Gateway and click **More** > **Delete** in the **Actions** column.
5. On the **NAT Gateway Details** page, click **Edit** next to the name. In the displayed dialog box, enter a new name and click **OK**. The name must be 2 to 128 characters in length and can contain numbers, hyphens (-) and underscores (_). It must start with a letter.
6. Click **Edit** next to the description. In the displayed dialog box, enter a new description and click **OK**. The description must be 2 to 256 characters in length and cannot start with http:// or https://.

2.3. Modify the specification of a NAT Gateway

This topic describes how to modify the specification of a NAT Gateway.

Context

NAT Gateway provides small, medium, large, and super large-1 specifications. You can select different specifications for NAT Gateway to adjust the performance metrics (Max Connections and CPS). However, data throughput is not affected by the specification. For more information, see Types of NAT gateway.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, find the target NAT Gateway and click **More** > **Delete** in the **Actions** column.
5. In the **Configuration Upgrade** area, select a new specification and then click **Pay**.

2.4. Delete a NAT Gateway

This topic describes how to delete a NAT Gateway.

Prerequisites

Before you delete a NAT Gateway, make sure that the following conditions are met:

- The NAT Gateway is not associated with an EIP. For more information, see Disassociate an EIP from a NAT Gateway.

- The DNAT table does not contain any DNAT entry. For more information, see Delete a DNAT entry.
- The SNAT table does not contain any SNAT entry. For more information, see Delete an SNAT entry.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, find the target NAT Gateway and click **More** > **Delete** in the **Actions** column.
5. 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, DNAT and SNAT entries in the NAT Gateway are deleted and EIPs are disassociated automatically.

3.Manage a DNAT table

3.1. DNAT table overview

NAT Gateway supports the Destination Network Address Translation (DNAT) feature. You can create DNAT entries to map public IP addresses to ECS instances in a Virtual Private Cloud (VPC) network. This way, the ECS instances can receive requests from the Internet.

DNAT entries

You can configure port mapping when you create a DNAT entry. After the DNAT entry is created, requests destined for the specified public IP address are forwarded to the ECS instances within a VPC network based on the port mapping rule.

Each DNAT entry consists of the following elements:

- **Public IP address**: the EIP associated with the NAT gateway.
- **Private IP address**: the private IP address assigned to the ECS instance in the VPC network.
- **Public Port**: the external port where requests from the Internet are received.
- **Private Port**: the internal port to which the requests received on the external port are forward ed.
- **Protocol Type**: the protocol used by the ports.

> Note If you have purchase a NAT service plan under your account before January 26, 2018, public IP addresses in the DNAT entry are provided by the NAT service plan.

Port mapping and IP mapping

The DNAT feature supports port mapping and IP mapping:

- Port mapping

  After port mapping is configured, a NAT gateway forwards requests destined for a public IP ad dress to the specified ECS instance based on the specified protocol and ports.

DNAT entry	Public IP add ress	Public port	Private IP ad dress	Private port	Protocol type
Entry 1	139.224.xx.xx	80	192.168.x.x	80	TCP
Entry 2	139.224.xx.xx	8080	192.168.x.x	8000	UDP

  Entry 1: The NAT gateway forwards requests destined for TCP port 80 of ECS instance 139.244. xx.xx to TCP port 80 of ECS instance 192.168.x.x.

  Entry 2: The NAT gateway forwards requests destined for UDP port 8080 of ECS instance 139.22 4.xx.xx to UDP port 8000 of ECS instance 192.168.x.x.

- IP mapping

  After IP mapping is configured, a NAT gateway forwards all requests destined for a public IP ad dress to the specified ECS instance.

DNAT entry	Public IP address	Public port	Private IP address	Private port	Protocol type
Entry 3	139.224.xx.xx	Any	192.168.x.x	Any	Any

Entry 3: The NAT gateway forwards requests destined for ECS instance 139.224.xx.xx to ECS instance 192.168.x.x.

3.2. Create a DNAT entry

This topic describes how to create a Destination Network Address Translation (DNAT) entry. Network Address Translation (NAT) Gateway supports DNAT. DNAT maps public IP addresses to private IP addresses of Elastic Compute Service (ECS) instances in a Virtual Private Cloud (VPC) network. This way, the ECS instances can receive inbound packets sent over the Internet. DNAT supports port mapping and IP mapping.

Prerequisites

A NAT gateway is created and associated with an Elastic IP address. For more information, see Create a NAT Gateway and Associate an EIP with a NAT Gateway.

> Note If you purchased a NAT bandwidth plan before January 26, 2018, you must ensure that there are unused public IP addresses in the NAT bandwidth plan.

Context

You cannot create DNAT entries for ECS instances that are associated with Elastic IP addresses.

To create a DNAT entry for such an ECS instance, you must disassociate the Elastic IP address from the ECS instance first. After you delete the association, you can create a DNAT entry for the ECS instance. For more information, see Unbind an Elastic IP address from a cloud instance and Create a DNAT entry.

> Note If an ECS instance is associated with an Elastic IP address, and the private IP address of the ECS instance is used in a DNAT entry of a NAT gateway, the ECS instance preferentially uses the Elastic IP address to access the Internet.

Procedure

1. Log on to the NAT Gateway console.
2. In the top navigation bar, select the region where the NAT gateway is deployed.
3. On the **NAT Gateways** page, find the target NAT gateway, and click **Configure DNAT** in the **Actions** column.
4. On the **DNAT Table** page, click **Create DNAT Entry**.
5. On the **Create DNAT Entry** page that appears, set the parameters as required, and click **OK**.

Parameter	Description

Parameter	Description
Public IP Address	Select an available public IP address. Note If a public IP address is already used in a SNAT entry, it cannot be used in a DNAT entry.
Private IP Address	Specify the private IP address of the ECS instance that uses the DNAT entry to receive inbound packets sent over the Internet. You can specify the private IP address of the ECS instance in the following ways: ○ **Auto Fill**: select the ECS instance from the ECS instance list or select the Elastic Network Interface (ENI) of the ECS instance from the ENI list. ○ **Manually Input**: enter the private IP address of the ECS instance. Note The CIDR block of the private IP address must be within that of the VPC network. You can also enter the private IP address of your ECS instance.
Port Settings	Select a DNAT mapping method: ○ **All**: IP mapping. All requests destined for the public IP address are forwarded to the target ECS instance. ○ **Specific Port**: port mapping. Requests received on a public port over a protocol are all forwarded to the specified internal port of the target ECS instance. After you select Specific Port, specify the **Public Port** (the external port), **Private Port** (the internal port), and **IP Protocol** (the protocol over which inbound packets are sent).
Entry Name	Enter a name for the DNAT entry. The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter.

Related information

- CreateForwardEntry

3.3. Modify a DNAT entry

You can modify the public IP address, private IP address, ports, and name of a DNAT entry.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, find the target NAT gateway, and click **Configure DNAT** in the **A**

ctions column.

5. On the **DNAT Table** page, find the target DNAT entry and click **Edit** in the **Actions** column.
6. On the **Edit DNAT Entry** page, modify the public IP address, private IP address, ports and nam e of the DNAT entry, and click **OK**.

3.4. Delete a DNAT entry

This topic describes how to delete a DNAT entry.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, find the target NAT gateway, and click **Configure DNAT** in the **A ctions** column.
5. On the **DNAT Table** page, find the target DNAT entry, and click **Remove** in the **Actions** colum n.
6. In the displayed dialog box, click **OK**.

4.Manage an SNAT table

4.1. Overview

NAT Gateways support the SNAT function. This function allows ECS instances that are not associated with public IP addresses in a VPC to access the Internet.

SNAT entries

You can create SNAT entries in a SNAT table to enable ECS instances to access the Internet.

Each SNAT entry consists of the following two parts:

- **VSwitch or ECS Instance**: The VSwitch or ECS instance that needs to use the SNAT function.
- **Public IP**: The public IP address used to grant access to the Internet.

> Note
>
> - You can select multiple public IP addresses to build a SNAT IP address pool. When a n ECS instance in a VPC initiates an Internet access request, the ECS instance uses a public IP address in the SNAT address pool to access the Internet.
> - If you purchased a NAT bandwidth package before January 26, 2018, the public IP ad dress is the IP address provided by the bandwidth package.

VSwitch granularity and ECS granularity

The SNAT function provides the following two types of granularity:

- VSwitch granularity

  If you select VSwitch granularity to create a SNAT entry, the NAT Gateway provides the Intern et proxy service for an ECS instance in the specified VSwitch when the ECS instance initiates a n Internet access request. In this way, the ECS instance can use the specified public IP address to access the Internet. By default, all ECS instances in the VSwitch can use the specified public IP address to access the Internet.

  > Note If an ECS instance is already associated with a public IP address (for example, it i s assigned a public IP address, associated with an EIP, or configured with DNAT IP mapping) , the ECS instance accesses the Internet by using the associated public IP address instead of the SNAT function of the NAT Gateway. To configure ECS instances in a VPC with the sa me public IP address, see Attach an ENI to an ECS that is allocated with an public IP addres s, Attach an ENI to an ECS instance associated with an EIP, and Attach an ENI to an ECS inst ance configured with DNAT IP mapping.

- ECS granularity

  If you select VSwitch granularity to create a SNAT entry, the specified ECS instance uses the sp ecified public IP address to access the Internet. When the ECS instance initiates an Internet acc ess request, the NAT Gateway provides the Internet proxy service for the ECS instance.

4.2. Create an SNAT entry

This topic describes how to create a Source Network Address Translation (SNAT) entry. SNAT allows Elastic Compute Service (ECS) instances in a Virtual Private Cloud (VPC) network to access the Internet without using public IP addresses.

Prerequisites

Before you create an SNAT entry, make sure that the following requirements are met:

- A NAT gateway is created and associated with an elastic IP address (EIP). For more information, see Create a NAT Gateway and Associate an EIP with a NAT Gateway.

  > Note If you purchased a NAT service plan before January 26, 2018, make sure that available public IP addresses are included in the NAT service plan.

- To create an SNAT entry with VSwitch granularity, make sure that the VSwitch is created and associated with the NAT gateway in a VPC network. For more information, see.
- To create an SNAT entry with ECS granularity, make sure that the ECS instance is created and associated with the NAT gateway in a VPC network. For more information, see.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, click **Configure SNAT** in the **Actions** column corresponding to the target NAT gateway.
5. On the **SNAT Table** page, click **Create SNAT Entry**.
6. In the **Create SNAT Entry** dialog box that appears, set the parameters. Click **OK**. The following table describes the parameters.

Parameter	Description
VSwitch Granularity	
VSwitch	Select the VSwitch for which you want to create the SNAT entry in the associated VPC. All ECS instances that belong to the specified VSwitch can access the Internet by using the SNAT function. Note If an ECS instance has a public IP address (for example, a fixed public IP address is assigned, an Elastic IP address is associated, or DNAT IP mapping is configured) and initiates an Internet access request, the instance preferentially accesses the Internet by using the public IP address instead of the SNAT function of NAT Gateway. To configure ECS instances in a VPC with the same public IP address, see Attach an ENI to an ECS that is allocated with an public IP address, Attach an ENI to an ECS instance associated with an EIP, and Attach an ENI to an ECS instance configured with DNAT IP mapping.
VSwitch CIDR Block	The CIDR block of the selected VSwitch.

Parameter	Description
Public IP	Select the public IP address that is used to access the Internet. You can select multiple public IP addresses to build a SNAT IP address pool. Note If you select multiple public IP addresses to build a SNAT IP address pool, you must ensure that each public IP address is added to the same shared bandwidth. The maximum bandwidth for each public IP address in an SNAT IP address pool is 200 Mbit/s. To make full use of Internet Shared Bandwidth and avoid port conflicts caused by insufficient public IP addresses, we recommend that you add public IP addresses in an SNAT rule as follows: ◦ If the peak bandwidth of the Internet Shared Bandwidth instance is 1024 Mbit/s, configure at least five public IP addresses in the SNAT rule. ◦ For each additional 200 Mbit/s of the peak bandwidth of the Internet Shared Bandwidth instance, at least one public IP address must be added in the SNAT rule. Note A public IP address that is already used in a DNAT entry cannot be used to create a SNAT entry.
Entry Name	Enter a name for the SNAT entry. The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
ECS Granularity	
Available ECS Instances	Select the ECS instance for which you want to create the SNAT entry in the associated VPC. The selected ECS instance will access the Internet by using the specified public IP address. Ensure that the following conditions are met: ◦ The ECS instance is running. ◦ The ECS instance is not associated with any public IP addresses or Elastic IP addresses.
ECS CIDR Block	The CIDR block of the ECS instance.

Parameter	Description
Public IP	Select the public IP address that is used to access the Internet. You can select multiple public IP addresses to build a SNAT IP address pool. Note If you select multiple public IP addresses to build a SNAT IP address pool, you must ensure that each public IP address is added to the same shared bandwidth. The maximum bandwidth for each public IP address in an SNAT IP address pool is 200 Mbit/s. To make full use of Internet Shared Bandwidth and avoid port conflicts caused by insufficient public IP addresses, we recommend that you add public IP addresses in an SNAT rule as follows: ○ If the peak bandwidth of the Internet Shared Bandwidth instance is 1024 Mbit/s, configure at least five public IP addresses in the SNAT rule. ○ For each additional 200 Mbit/s of the peak bandwidth of the Internet Shared Bandwidth instance, at least one public IP address must be added in the SNAT rule. Note A public IP address that is already used in a DNAT entry cannot be used to create a SNAT entry.
Entry Name	Enter a name for the SNAT entry. The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.

Related information

- CreateSnatEntry

4.3. Modify an SNAT entry

You can modify the public IP address and name of an SNAT entry.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, click **Configure SNAT** in the **Actions** column corresponding to the target NAT gateway.
5. On the **SNAT Table** page, find the target SNAT entry and click **Edit** in the **Actions** column.

6. On the **Edit SNAT Entry** page, modify the public IP address and name of the SNAT entry and c lick **OK**.

4.4. Delete an SNAT entry

This topic describes how to delete an SNAT entry.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, click **Configure SNAT** in the **Actions** column corresponding to th e target NAT gateway.
5. On the **SNAT Table** page, find the target SNAT entry and click **Remove** in the **Actions** column.
6. In the displayed dialog box, click **OK**.

5.Manage EIPs

5.1. Associate an EIP with a NAT Gateway

This topic describes how to associate an Elastic IP Address (EIP) with a NAT Gateway. A NAT Gateway is essentially an Internet gateway which requires public IP addresses to function. After creating a NAT Gateway, you can associate one or more Elastic IP Addresses (EIPs) with the NAT Gateway.

Prerequisites

Before you associate an EIP with a NAT Gateway, make sure that the following conditions are met:

- No NAT bandwidth package was purchased before 23:59 January 26, 2018.

  If you have created a NAT bandwidth package for a NAT Gateway before 23:59 January 26, 2018, you still need to use the bandwidth package to associate public IP addresses with the NAT Gateway. To associate an EIP with a NAT Gateway, follow the steps in Why am I unable to associate an EIP with a NAT Gateway in the NAT Gateway console.

- A NAT Gateway and an EIP are created. For more information, see Create a NAT Gateway and Purchase a new Elastic IP address.

Context

A NAT Gateway can be associated with up to 20 EIPs, among which no more than ten are billed based on traffic. The peak bandwidth of each EIP that is billed based on traffic cannot exceed 200 Mbps. You can request a quota increase on the Quota Management page in the console. For more information, see Manage quotas.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, find the target NAT Gateway and choose **More** > **Bind Elastic IP Address** in the **Actions** column.
5. On the **Bind Elastic IP Address** page, complete the following configurations, and then click **OK**.

Category	Configuration	Description
	Usable EIP list	Select an EIP that is used to access the Internet.

Category	Configuration	Description
Select from EIP list	VSwitch	Select the VSwitch to which you want to add SNAT entries. The system automatically adds SNAT entries so that Alibaba Cloud services connected to this VSwitch can access the Internet. Alternatively, you can skip this step and add SNAT entries after you associate an EIP with the NAT Gateway. For more information, see 创建SNAT条目. Note This option is only available for the NAT Gateways that are not associated with an EIP.
Allocate one EIP and bind it to NAT Gateway	Buy EIP	Displays the number of EIPs to be purchased. The default value is 1 and cannot be modified. The system automatically creates an EIP billed by traffic and associates it with the NAT Gateway.

Related information

- AssociateEipAddress

5.2. Disassociate an EIP from a NAT Gateway

This topic describes how to disassociate an EIP from a NAT Gateway.

Prerequisites

Make sure that the EIP to be disassociated is not used by any SNAT or DNAT entry.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.

4. On the **NAT Gateways** page, find the target NAT Gateway and click **More** > **Unbind Elastic IP Address** in the **Actions** column.
5. On the **Unbind Elastic IP Address** page, select the target EIP and click **OK**.

6.Service-linked roles for NAT Gateway

This topic describes the service-linked role AliyunServiceRoleForNatgw for NAT Gateway and how to delete the service-linked role for NAT Gateway.

What is a service-linked role?

A service-linked role is a Resource Access Management (RAM) role that can only be assumed by the linked service. If you want to use a feature of an Alibaba Cloud service, you must have permissions on the Alibaba Cloud service. Service-linked roles help you add the permissions for the Alibaba Cloud services and prevent user errors. For more information, see Service linked roles.

Create a service-linked role for NAT Gateway

When you create an enhanced NAT gateway that does not have a service-linked role, the system automatically creates the service-linked role AliyunServiceRoleForNatgw for the NAT gateway. Then, it adds the permission policy AliyunServiceRolePolicyForNatgw to the role. This allows the NAT gateway to access other resources on Alibaba Cloud. The following shows the content of the permission policy:

> **Note** When you create a normal NAT gateway, the system does not create the service-linked role AliyunServiceRoleForNatgw for the NAT gateway.

```
{
"Version": "1",
"Statement": [
{
"Action": [
"vpc:DescribeVSwitchAttributes"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": [
"ecs:CreateNetworkInterface",
"ecs:CreateSecurityGroup",
"ecs:AuthorizeSecurityGroup",
"ecs:RevokeSecurityGroup",
"ecs:DeleteSecurityGroup",
"ecs:JoinSecurityGroup",
"ecs:DeleteSecurityGroup",
"ecs:LeaveSecurityGroup",
"ecs:DescribeSecurityGroups"
```

```
"ecs:DescribeSecurityGroups",
"ecs:AttachNetworkInterface",
"ecs:DetachNetworkInterface",
"ecs:DeleteNetworkInterface",
"ecs:DescribeNetworkInterfaces",
"ecs:CreateNetworkInterfacePermission",
"ecs:DescribeNetworkInterfacePermissions",
"ecs:DeleteNetworkInterfacePermission",
"ecs:CreateSecurityGroupPermission",
"ecs:AuthorizeSecurityGroupPermission",
"ecs:RevokeSecurityGroupPermission",
"ecs:DeleteSecurityGroupPermission",
"ecs:JoinSecurityGroupPermission",
"ecs:DeleteSecurityGroupPermission",
"ecs:LeaveSecurityGroupPermission",
"ecs:DescribeSecurityGroupPermissions",
"ecs:AttachNetworkInterfacePermissions",
"ecs:DetachNetworkInterfacePermissions"
],
"Resource": "*",
"Effect": "Allow"
},
{
"Action": "ram:DeleteServiceLinkedRole",
"Resource": "*",
"Effect": "Allow",
"Condition": {
"StringEquals": {
"ram:ServiceName": "nat.aliyuncs.com"
}
}
}
]
}
```

Delete the service-linked role for NAT Gateway

If you want to delete the service-linked role AliyunServiceRoleForNatgw for NAT Gateway, you must first delete the NAT gateway that is linked with the role. For more information, see the following topics:

- Delete a NAT Gateway
- Delete a service linked role

7.Anti-DDoS Basic

Distributed Denial of Service (DDoS) attack is a malicious network attack against the target system, which can make the attacked network inaccessible. Alibaba Cloud provides up to 5 Gbit/s of basic anti-DDoS protection for NAT Gateway, which can efficiently prevent DDoS attack.

How Anti-DDoS Basic works

After you enable Anti-DDos Basic, all traffic from the Internet must first pass through Alibaba Cloud Security before arriving at NAT Gateway. Anti-DDoS Basic scrubs and filters common DDoS attacks at Alibaba Cloud Security. Anti-DDos Basic protects your services against attacks such as SYN flood, UDP flood, ACK flood, ICMP flood, and DNS Query flood.

Anti-DDoS Basic sets the scrubbing threshold and black hole triggering threshold based on 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 matc hes certain attack traffic pattern, Alibaba Cloud Security starts scrubbing the attack traffic. Th e scrubbing includes packet filtering, bandwidth capping, and traffic throttling.
- Blackholing: When the attack traffic from the Internet exceeds the black hole triggering thres hold, blackholing is triggered and all inbound traffic is dropped.

Scrubbing threshold

The thresholds for triggering traffic scrubbing and blackholing on NAT Gateway are calculated as described in the following table:

EIP bandwidth	Traffic scrubbing threshold (bits/s)	Traffic scrubbing threshold (packets/s)	Default black hole triggering threshold
Lower than or equal to 800 Mbit/s	800Mbps	120,000	1.5 Gbps
Higher than 800 Mbit/s	Predefined bandwidth	Predefined bandwidth × 150	Predefined bandwidth × 2

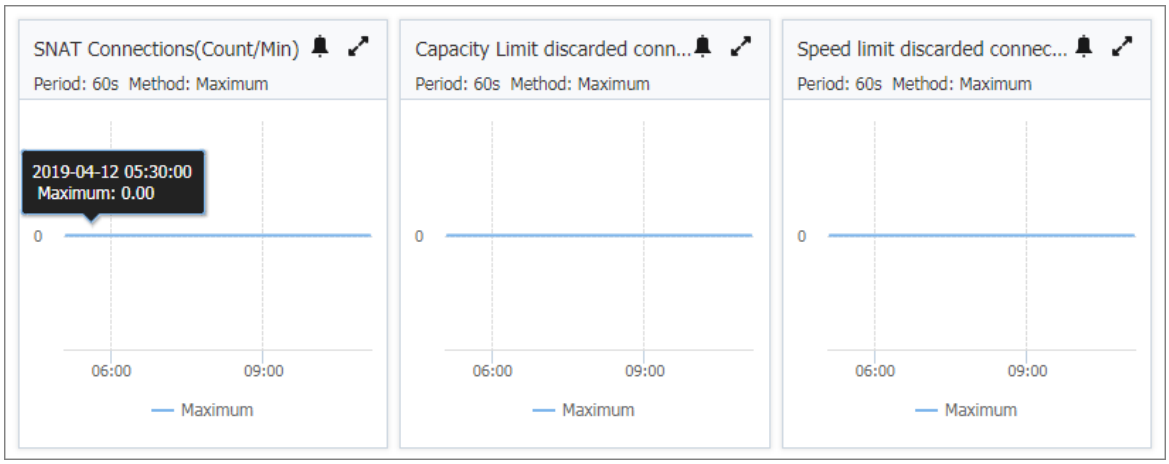
If the EIP bandwidth is 1,000 Mbit/s, the traffic scrubbing threshold (bits/s) is 1,000 Mbit/s, the traffic scrubbing threshold (packets/s) is 150,000 and the default blackholing threshold is 2 Gbit/s.

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. In the left-side navigation pane, click **NAT Gateways**.
3. In the top navigation bar, select the region of the NAT Gateway.
4. On the **NAT Gateways** page, find the target NAT Gateway and click the icon in the **SNAT Connections** column.



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

Item	Description	Dimension	Unit	Minimum monitoring granularity
SNAT connections	The number of 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
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

9.Manage quotas

You can query current quota usage in 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 NAT Gateways under your account.
4. To increase your resource quota, click **Apply** in the **Actions** column.
   - **Quantity for Application**: the number of resources you require. You must enter a number that is greater 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.