ALIBABA CLOUD

Alibaba Cloud

NAT Gateway

Common Configurations

Document Version: 20220209

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.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.

What is a service-linked role?

A service-linked role is a Resource Access Management (RAM) role that can be assumed by only the linked service. An Alibaba Cloud service may need to access other services to use a specific feature. Before you access a service, make sure that you are authorized to access the service.Service-linked roles simplify the authorization process and avoid risks caused by user errors. For more information, see Service-linked roles.

Create a service-linked role

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, the system attaches 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 standard NAT gateway, the system does not automatically 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: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

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:

1. Delete a NAT gateway
2. Delete a service-linked role

FAQ

Why is the service-linked role AliyunServiceRoleForNatgw for NAT Gateway not automatically created for a RAM user?

The service-linked role AliyunServiceRoleForNatgw for NAT Gateway is automatically created or deleted only when a RAM user has the required permissions. To acquire the permissions to create the service-linked role AliyunServiceRoleForNatgw for NAT Gateway, you must attach the following policy to the RAM user:

```
{
    "Statement": [
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "nat.aliyuncs.com"
                }
            }
        }
    ],
    "Version": "1"
}
```

Related information

- Service-linked roles

2.Anti-DDoS Origin Basic

A distributed denial-of-service (DDoS) attack is a malicious network attack against one or more systems, which can crash the targeted network. Alibaba Cloud provides up to 5 Gbit/s of basic anti-DDoS protection for a NAT gateway free of charge. Anti-DDoS Origin Basic can effectively prevent DDoS attacks.

How Anti-DDoS Origin Basic works

After you enable Anti-DDoS Origin Basic, traffic from the Internet must pass through Alibaba Cloud Security before the traffic arrives at the NAT gateway. Anti-DDoS Origin Basic scrubs and filters common DDoS attacks at Alibaba Cloud Security. Anti-DDoS Origin Basic protects your services against attacks such as SYN floods, UDP floods, ACK floods, ICMP floods, and DNS Query floods.

Anti-DDoS Origin Basic specifies the traffic scrubbing and blackhole triggering thresholds based on the bandwidth limit of the elastic IP address (EIP) that is associated with the NAT gateway. When the inbound traffic reaches the threshold, traffic scrubbing or blackhole is triggered:

- Traffic scrubbing: When the attack traffic from the Internet exceeds the scrubbing threshold or matches the attack traffic pattern, Alibaba Cloud Security starts to scrub the attack traffic. Traffic scrubbing includes packet filtering, bandwidth capping, and traffic throttling.
- Blackhole: When the attack traffic from the Internet exceeds the blackhole triggering threshold, blackhole is triggered and all inbound traffic is dropped.

Traffic scrubbing and blackhole triggering thresholds

The following table describes the methods that are used to calculate the traffic scrubbing and blackhole triggering thresholds on NAT gateways.

Bandwidth limit of the EIP	Traffic scrubbing threshold (bit/s)	Traffic scrubbing threshold (pps)	Default blackhole triggering threshold
Lower than or equal to 800 Mbit/s	800 Mbit/s	120,000	1.5 Gbit/s
Higher than 800 Mbit/s	Predefined bandwidth	Predefined bandwidth × 150	Predefined bandwidth × 2

If the bandwidth limit of the EIP is 1,000 Mbit/s, the traffic scrubbing threshold (bit/s) is 1,000 Mbit/s, the traffic scrubbing threshold (pps) is 150,000, and the default blackhole triggering threshold is 2 Gbit/s.

3.Manage quotas

This topic describes how to manage the quota usage of NAT gateways in the Virtual Private Cloud (VPC) console. You can request a quota increase if the remaining resources cannot meet the business requirements.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, choose **O&M and Monitoring > Quota Management**.
3. On the **Quota Management** page, click the **NAT Gateway** tab to view the quota usage of the current Alibaba Cloud account.
4. To request a quota increase, click **Submit Application** in the **Actions** column.
5. In the **Apply** dialog box, set the following parameters and submit the application.
    - **Requested Value**: Enter the requested value.
    - **Reason**: Enter detailed reasons for the application, including the scenarios and necessity.
    - **Email**: Enter the email address of the applicant.
6. Click **OK**.

    The system automatically reviews your quota increase application. You can check whether your application is approved based on the status of the application: If the status is **Rejected**, your application is rejected. If the status is **Approved**, your application is approved, and the quota is automatically raised to the specified amount.