ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

NAT Gateway

Developer Guide

Product Version: v3.16.2

Document Version: 20220902

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.Getting started

1.1. Usage notes on development documentation

This topic describes how to view the desired product development documentation when you use Apsara Stack API (ASAPI).

Prerequisites

The Apsara Stack version is obtained from an O&M personnel or operations administrator.

Procedure

You can go to the Apsara Stack documentation center and view the desired product documentation.

1. Go to the Apsara Stack Documentation Center page by using a browser.
2. Click the **Enterprise**, **Agility**, or **All-in-one** tab based on the Apsara Stack version that you use.
3. Select an Apsara Stack version from the drop-down list.
4. In the left-side navigation pane, select the name of the product that you want to view.
5. In the upper-right corner of the product documentation section, click **View Details** or **Download PDF**.

1.2. Call an API operation

Apsara Stack allows you to call API operations by using the Portable OpenAPI Proxy (POP) gateway or the Apsara Stack API (ASAPI) gateway. To ensure that Apsara Stack

> **Note**
>
> You can still use the ASAPI gateway to call API operations. For more information, see Call API operations by using the ASAPI gateway, Obtain the endpoint of ASAPI, an

Procedure

1. Obtain AccessKey credentials.

   Obtain the AccessKey credentials that are required when you call an API operation. For more information, see Obtain an AccessKey pairor Obtain an STS AccessKey 3-tuple.

   > **Note**
   >
   > We recommend that you use the AccessKey pair of a personal account assigned by RAM or STS credentials to call the API operations of the Apsara Uni-manager Management Console and cloud services.

2. Obtain the region ID.

   For more information, see Obtain the values of common header parameters.

3. Obtain the organization ID and resource set ID.

   You must call an API operation to obtain an organization ID. For more information about how to obtain organization IDs, see the *GetOrganizationList* section in *Apsara Uni-manager Management Console Developer Guide*.

   You must call an API operation to obtain a resource set ID. For more information about how to obtain resource set IDs, see the *ListResourceGroup* section in *Apsara Uni-manager Management Console Developer Guide*.

   > **Note**
   >
   > When you call an API operation, set the `<x-acs-organizationid>` parameter to the organization ID that you obtained, and set the `<x-acs-resourcegroupid>` parameter to the resource set ID that you obtained. This way, you can query resources in the specified organization and resource set.
   >
   > - If you do not set the `<x-acs-organizationid>` parameter, the resources in the organization to which the current user belongs are queried.
   > - If you do not set the `<x-acs-resourcegroupid>` parameter, this parameter is left empty by default. If you specify a resource set ID, you must also specify an organization ID.

4. Obtain the developer guide for reference.

   Obtain the developer guide of the cloud service that you want to use. You can learn the features of API operations and how to call the API operations. For more infc

5. Obtain the endpoint of the cloud service.
6. Obtain an SDK of the cloud service and call an API operation.

2.Preparations

2.1. Log on to the API Tool console

You can log on to the API Tool console from the Apsara Uni-manager Management Console.

Prerequisites

- Before you log on to the Apsara Uni-manager Management Console, the endpoint of the console is obtained from the deployment personnel.
- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Enter the URL of the Apsara Uni-manager Management Console in the address bar and press Enter.
2. Enter your username and password.

   Obtain the username and password that are used to log on to the Apsara Uni-manager Management Console from the operations administrator.

   > **Note** When you log on to the Apsara Uni-manager Management Console for the first time, you must change the password of your account. For security purposes, your password must meet the minimum complexity requirements. The password must be 10 to 32 characters in length and must contain at least two of the following character types:
   >
   > - Uppercase or lowercase letters
   > - Digits
   > - Special characters, which include ! @ # $ %

3. Click **Log On**.
4. If your account has multi-factor authentication (MFA) enabled, perform corresponding operations in the following scenarios:
   - You log on to the Apsara Uni-manager Management Console for the first time after MFA is enabled by the administrator.
     a. On the Bind Virtual MFA Device page, bind an MFA device.
     b. Enter the username and password again as in Step 2 and click **Log On**.
     c. Enter a six-digit MFA verification code and click **Authenticate**.
   - You have enabled MFA and bound an MFA device.

     Enter a six-digit MFA verification code and click **Authenticate**.

     > **Note** For more information, see the *Bind a virtual MFA device to enable MFA* topic in *Apsara Uni-manager Management Console User Guide*.

5. In the top navigation bar, choose **Products > Others > API Tool**.

2.2. Obtain API information

To call API operations by using an SDK, you must first obtain information about the service name, API operation name, and API version.

Context

The information on the API Directory page of the Apsara Uni-manager Management Console is for reference only. For more information about how to call API operations, see the developer guides of cloud services. If the information on the API Directory page is different from that in the developer guide of a cloud service, the information in the developer guide prevails.

Procedure

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, click **Products** and choose **Others** > **API Tool**.
3. In the left-side navigation pane, click **API Directory**.
4. On the **API Directory** page, select the required cloud service from the Product Name drop-down list, enter a keyword of an operation name in the search box, and then click Search.
5. In the search result, you can view the **cloud service name**, **API operation name**, and **API version**.

2.3. Obtain AccessKey credentials

AccessKey credentials are assigned by Resource Access Management (RAM) or Security Token Service (STS). You can use one type of AccessKey credentials for authentication when you call API operations. This topic describes how to obtain an AccessKey pair that is assigned by RAM.

Context

An AccessKey pair is used to verify the identity of request senders. An AccessKey pair consists of an AccessKey ID and an AccessKey secret that are used to implement symmetric encryption. The AccessKey ID is used to identify a user. The AccessKey secret is used to encrypt the signature string.

You can use RAM or STS to assign AccessKey credentials:

- An AccessKey pair that is assigned by RAM to a third party consists of an AccessKey ID and an AccessKey secret.
- An AccessKey 3-tuple that is assigned by STS to a third party consists of an AccessKey ID, an AccessKey secret, and a security token. For more information, see Obtain an STS AccessKey 3-tuple.

The Apsara Uni-manager Management Console provides AccessKey pairs for personal accounts or organizations. Only the administrators of level-1 organizations and operations administrators can obtain the AccessKey pairs of organizations. We recommend that you use the AccessKey pairs of personal accounts to call the operations provided by the Apsara Uni-manager Management Console and cloud services. If you use the AccessKey pair of a personal account, configure the header parameters that are described in the following table for access control. Otherwise, an error that indicates insufficient permissions can occur.

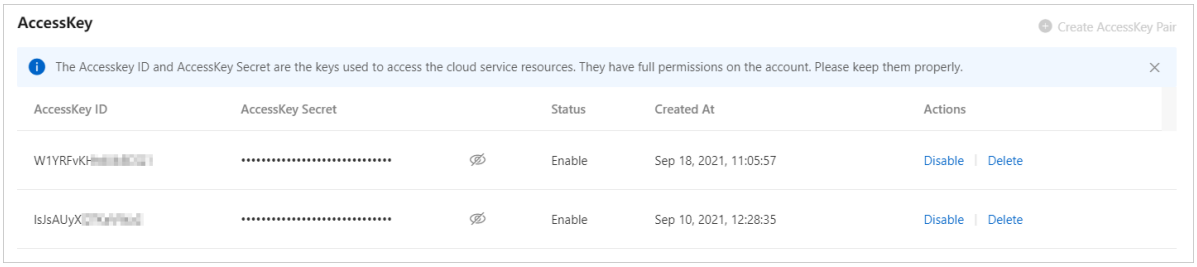
Warning The AccessKey pair of a personal account is managed and controlled by the permission system of the Apsara Uni-manager Management Console. If you need to obtain the AccessKey pair of an organization, make sure that your operation is allowed by an administrator. This ensures security.

Parameter	Overview
x-acs-regionid	The ID of the region. Example: cn-hangzhou-*.
x-acs-organizationid	The ID of the organization in the Apsara Uni-manager Management Console. For more information about how to obtain organization IDs, see the *GetOrganizationList* section in *Apsara Uni-manager Management Console Developer Guide*.
x-acs-resourcegroupid	The ID of the resource set in the Apsara Uni-manager Management Console. For more information about how to obtain resource set IDs, see the *ListResourceGroup* section in *Apsara Uni-manager Management Console Developer Guide*.
x-acs-instanceid	The ID of the instance that you want to manage. If you want to obtain the ID of an Elastic Compute Service (ECS) instance, you can obtain the ID from the ECS instance list.

Obtain the AccessKey pair of a personal account

To obtain the AccessKey pair of a personal account, perform the following steps:

1. Log on to the Apsara Uni-manager Management Console.
2. Click the profile picture in the upper-right corner of the page and click **User Information**.
3. In the **AccessKey Pair** section, view the AccessKey pair of the personal account.



Note An AccessKey pair consists of an AccessKey ID and an AccessKey secret. These credentials provide full permissions on cloud resources within your account. You must keep the AccessKey pair confidential.

Obtain the AccessKey pair of an organization

To obtain the AccessKey pair of an organization, perform the following steps:

1. Log on to the Apsara Uni-manager Management Console as an administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources > Organizations**.
4. In the organization list, click the name of the level-1 organization whose AccessKey pair you want to obtain.
5. Click **Management AccessKey** on the right side of the page.
6. In the dialog box that appears, view the AccessKey pair of the organization.

2.4. Obtain an STS AccessKey 3-tuple

This topic describes how to use Security Token Service (STS) to call API operations in Apsara Stack.

Background information

STS allows you to manage temporary credentials to your Apsara Stack resources. You can use STS to call API operations in Apsara Stack.

An STS AccessKey 3-tuple consists of an AccessKey ID, an AccessKey secret, and a security token. When you use STS to call API operations, you must specify an STS AccessKey 3-tuple. For more information about STS, see What is STS.

Procedure

1. Obtain the `RAM role`.
   i. Log on to the Apsara Uni-manager Management Console.
   ii. Click the profile picture in the upper-right corner of the page and click **User Information**.
   iii. Click **View Current Role Policy**.

   In the **View Policies of Current Role** dialog box, view your `RAM role`.
2. Obtain the STS AccessKey 3-tuple.

> **Note**
>
> In the following code, replace the parameters with your actual information. Delete the angle brackets (<>) before you submit the code.
>
> The following section describes the parameters:
>
> - <yourRegionID>: Replace the parameter with the region ID.
> - <yourAccessKeyID>: Replace the parameter with your AccessKey ID.
> - <yourAccessKeySecret>: Replace the parameter with your AccessKey secret.
> - <yourRoleSessionName>: Replace the parameter with the name of the current session.
> - <yourRoleArn>: Replace the parameter with your RAM role.
> - <sts.aliyuns.com>: Replace the parameter with the STS endpoint.

```
public static void main(String[] args) {
    // Create a DefaultAcsClient instance and initialize it.
    // Specify the region ID, AccessKey ID, and AccessKey secret.
    DefaultProfile profile = DefaultProfile.getProfile("<yourRegionID>", "<yourAccessKeyID>", "<yourAccessKeySecret>");
    HttpClientConfig clientConfig = HttpClientConfig.getDefault();
    clientConfig.setIgnoreSSLCerts(true);
    clientConfig.setProtocolType(ProtocolType.HTTPS);
    profile.setHttpClientConfig(clientConfig);
    IAcsClient client = new DefaultAcsClient(profile);
    String assumeRole = callAssumeRole(client);
    if (StringUtils.isEmpty(assumeRole)) return;
    JSONObject assumeRoleJson = JSONObject.parseObject(assumeRole);
    JSONObject credentials = assumeRoleJson.getJSONObject("Credentials");
    // Obtain the STS AccessKey 3-tuple.
    String stsAK = credentials.getString("AccessKeyId");
    String stsSK = credentials.getString("AccessKeySecret");
    String stsToken = credentials.getString("SecurityToken");
}

private static String callAssumeRole(IAcsClient client) {
    CommonRequest request = new CommonRequest();
    // Replace "sts.aliyuns.com" with the endpoint of STS. The format of an STS endpoint is sts-vpc.${global:region}.${global:internet-domain}.
    request.setSysDomain("sts.aliyuns.com");
    request.setSysProduct("Sts");
    request.setSysAction("AssumeRole");
    request.setSysVersion("2015-04-01");
    request.setSysMethod(MethodType.POST);
    request.setHttpContentType(FormatType.FORM);
    // Replace "<yourRoleSessionName>" with the name of the current session.
    request.putQueryParameter("RoleSessionName", "<yourRoleSessionName>");
    // Replace "<yourRoleArn>" with the actual ARN that you obtain in the preceding step for the RAM role.
    request.putQueryParameter("RoleArn", "<yourRoleArn>");
    try {
        CommonResponse response = client.getCommonResponse(request);
        return response.getData();
    } catch (ServerException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    } catch (ClientException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    }
    return null;
}
```

3. Use the STS AccessKey 3-tuple to call an API operation of a cloud service. The following sample code provides an example on how to call the `DescribeNatGateways` operation of NAT Gateway.

> **Note**
>
> In the following code, replace the parameters with your actual information. Delete the angle brackets (<>) before you submit the code.
>
> The following section describes the parameters:
>
> - <yourRegionID>: Replace the parameter with the region ID.
> - <yourStsAccesskeyID>: Replace the parameter with your STS AccessKey ID.
> - <yourStsAccessKeySecret>: Replace the parameter with your STS AccessKey secret.
> - <yourStsToken>. Replace the parameter with your security token.
> - <yourResourceGroupID>: Replace the parameter with the resource set ID.
> - <yourOrganizationID>: Replace the parameter with the organization ID.

```
public static void main(String[] args) {
    // Replace "<yourRegionID>" with the region ID.
    // Replace "<yourStsAccessKeyID>" and "<yourStsAccessKeySecret>" with the AccessKey ID and AccessKey secret of the 3-tuple obtained in the pr
evious step.
    DefaultProfile profile = DefaultProfile.getProfile("<yourRegionID>", "<yourStsAccesskey>", "<yourStsAccessSecret>");
    HttpClientConfig clientConfig = HttpClientConfig.getDefault();
    clientConfig.setIgnoreSSLCerts(true);
    clientConfig.setProtocolType(ProtocolType.HTTPS);
    profile.setHttpClientConfig(clientConfig);
    IAcsClient client = new DefaultAcsClient(profile);
    CommonRequest request = new CommonRequest();
    request.setSysDomain("vpc.aliyuns.com");
    request.setSysProduct("Vpc");
    request.setSysAction("DescribeNatGateways");
    request.setSysVersion("2016-04-28");
    request.setSysMethod(MethodType.POST);
    request.setHttpContentType(FormatType.FORM);
    // Replace "<yourRegionID>" with the region ID.
    request.putHeaderParameter("x-acs-regionid", "<yourRegionID>");
    // Replace "<yourStsToken>" with the security token of the 3-tuple obtained in the previous step.
    request.putQueryParameter("SecurityToken", "<yourStsToken>");
    // Optional. Replace the parameter with the resource set ID.
    // request.putHeaderParameter("x-acs-resourcegroupid", "<yourResourceGroupID>");
    // Required. Replace the parameter with the organization ID.
    request.putHeaderParameter("x-acs-organizationid", "<yourOrganizationID>");
    try {
        CommonResponse response = client.getCommonResponse(request);
        System.out.println(response.getData());
    } catch (ServerException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    } catch (ClientException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    }
}
```

2.5. Obtain the values of common header parameters

You must set header parameters when you call API operations. This topic describes the header parameters and how to obtain the values of the parameters. This topic also describes the return values of some parameters after you call API operations.

Header parameters

Parameter	Description
x-acs-regionid	The region ID. For more information, see Obtain a region ID.
x-acs-organizationid	The ID of the organization in the Apsara Uni-manager Management Console. For more information, see Obtain an organization ID.
x-acs-resourcegroupid	The ID of the resource set in the Apsara Uni-manager Management Console. For more information, see Obtain a resource set ID.
x-acs-instanceid	The ID of the instance that you want to manage. For more information, see Obtain an instance ID.

Obtain a region ID

1. Log on to the Apsara Uni-manager Management Console as an administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources** > **Regions**.
4. Click the name of the organization that you want to view.
5. View the region ID in the **Regions** section on the right.

Obtain an organization ID

You must call an operation to obtain an organization ID. For more information about how to obtain organization IDs, see the *GetOrganizationList* section in *Apsara Uni-manager Management Console Developer Guide*.

Obtain a resource set ID

You must call an operation to obtain a resource set ID. For more information about how to obtain resource set IDs, see the *ListResourceGroup* section in *Apsara Uni-manager Management Console Developer Guide*.

Obtain an instance ID

You can obtain the ID of an instance in the cloud service console of the Apsara Uni-manager Management Console. For example, to obtain the ID of a NAT gateway, perform the following steps:

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products** > **Networking** > **Virtual Private Cloud**.
3. In the left-side navigation pane, click **NAT Gateways**.
4. On the **NAT Gateways** page, view **instance IDs/names**.

Response parameters

The following response parameters are returned by default when you call operations to query the instances of cloud services.

Parameter	Description
ResourceGroupName	The name of the resource set.
ResourceGroup	The ID of the resource set.
DepartmentName	The name of the organization.
Department	The ID of the organization.

2.6. Obtain the endpoints of NAT Gateway

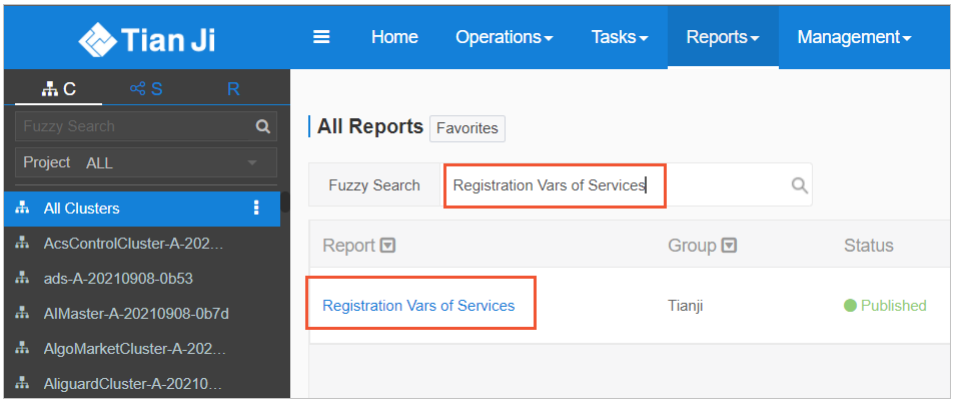
This topic describes how to obtain the endpoint of NAT Gateway.

Background information

When you call Apsara Stack API operations by using the Portable OpenAPI Proxy (POP) gateway, you must obtain the endpoint of your cloud service. You can obtain a service endpoint from an Apsara Stack onsite O&M engineer or by performing the following operations:

Procedure

1. Log on to Apsara Infrastructure Management.
   i. Log on to the Apsara Uni-manager Operations Console.
   ii. In the top navigation bar, choose **Products** > **Platforms** > **Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, click **Reports**.
3. On the **All Reports** page, search for `Registration Vars of Services` and click the report name.



4. On the **Registration Vars of Services** page, click the icon next to **Service** and search for `VPC`.

> **Note**
> NAT Gateway uses the Virtual Private Cloud (VPC) API.

5. Find `vpc-yaochi`. Right-click the value in the **Service Registration** column and select **Show More**.

   On the **Details** page, view the value of **vpc-internal.openapi.endpoint**. The value indicates the `endpoint` of NAT Gateway.

2.7. Obtain VPC SDK to use NAT gateways

When you call Apsara Stack API operations by using the Portable OpenAPI Proxy (POP) gateway, you must use an SDK of your cloud service. This topic describes how to obtain Alibaba Cloud SDK.

Background information

To use NAT gateways, you must install Virtual Private Cloud (VPC) SDK and the Alibaba Cloud core library. For example, to use VPC SDK for Java, you must download `aliyun-java-sdk-vpc` and `aliyun-java-sdk-core`.

- VPC SDK encapsulates the API released on April 28, 2016. The SDK identifies callers based on their AccessKey pairs and provides features such as automatic signing to allow you to create and manage resources by calling API operations. Alibaba Cloud SDK includes code and examples. You can create cloud applications by using an SDK in the programming language that you require.
- We recommend that you use the SDK core library that is provided on the Alibaba Cloud official website. The SDK core library is ideal for all cloud services and is compatible with Apsara Stack.

Instructions

Alibaba Cloud SDK supports Java, Python, and Go. You can select an SDK from Alibaba Cloud SDK based on your business requirements.

> **Note**
>
> We recommend that you use an SDK for Java, Python, or Go. If you use SDKs in other programming languages, the SDKs may be incompatible with your system.

3.Call examples for SDK for Java

3.1. Quick start

This topic describes how to obtain and use Virtual Private Cloud (VPC) SDK for Java. To use the features of NAT Gateway, you must use VPC SDK.

Environment preparation

- An authorized Apsara Stack account and an AccessKey pair are obtained. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. For more information, see Obtain an AccessKey pair.
- The endpoint of NAT Gateway is obtained. For more information, see Obtain the endpoint of NAT Gateway.
- Java Development Kit (JDK) 1.8 or later is installed. Alibaba Cloud SDK for Java requires JDK 1.8 or later.

Install VPC SDK for Java

If you use Apache Maven to manage Java projects, you need to only add Maven commands to the pom.xml file of the projects.

To use VPC SDK, you must install the SDK core library and VPC SDK. We recommend that you use the core library version 4.5.17 or later, and use the SDK version 3.2.0.

```
<dependencies>
        <dependency>
            <groupId>com.aliyun</groupId>
            <artifactId>aliyun-java-sdk-core</artifactId>
            <version>4.5.17</version>
        </dependency>
        <dependency>
            <groupId>com.aliyun</groupId>
            <artifactId>aliyun-java-sdk-vpc</artifactId>
            <version>3.2.0</version>
        </dependency>
</dependencies>
```

Use VPC SDK for Java

To use VPC SDK for Java, perform the following steps:

1. Create and initialize a DefaultAcsClient instance.
2. Create an API request and set the required parameters.
3. Initiate the API request and process the response or exception.

> **Note**
>
> In the following code, replace the parameters with your actual information. Delete the angle brackets (<>) in the final code.
>
> The following section describes the parameters:
>
> - <yourRegionID>: Replace the parameter with the region ID.
> - <yourAccessKeyID>: Replace the parameter with your AccessKey ID.
> - <yourAccessKeySecret>: Replace the parameter with your AccessKey secret.
> - <Product>: Replace the parameter with the name of the current service.
> - <Endpoint>: Replace the parameter with the endpoint of the current service.
> - <readTimeout>: Replace the parameter with a read timeout period based on your business requirements. Unit: milliseconds.
> - <connectionTimeout>: Replace the parameter with a connection timeout period based on your business requirements. Unit: milliseconds.
> - <maxRequestsPerHost>: Replace the parameter with the maximum number of requests that are supported by each host.
> - <maxRequests>: Replace the parameter with the maximum number of requests.
> - <http://192.168.XX.XX:33XX>: Replace the parameter with the IP address and port of the proxy.

```
import com.aliyuncs.http.HttpClientConfig;
import com.aliyuncs.http.ProtocolType;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.vpc.model.v20160428.*;
import com.google.gson.Gson;
public class Main {
     public static void main(String[] args) {
        // Create a DefaultAcsClient instance and initialize the instance.
        DefaultProfile profile = DefaultProfile.getProfile(
            "<yourRegionID>",          // Replace the parameter with the region ID.
            "<yourAccessKeyID>",      // Replace the parameter with your AccessKey ID.
            "<yourAccessKeySecret>"); // Replace the parameter with your AccessKey secret.
        // Specify the endpoint of the service.
        profile.addEndpoint("<yourRegionID>", "<Product>", "<Endpoint>");
        // Configure the request parameters.
        HttpClientConfig clientConfig = HttpClientConfig.getDefault();
        clientConfig.setIgnoreSSLCerts(true);// Ignore this parameter.
        clientConfig.setReadTimeoutMillis(<readTimeout>);// Optional. Specify the read timeout period. Unit: milliseconds.
        clientConfig.setConnectionTimeoutMillis(<connectionTimeout>);// Optional. Specify the connection timeout period. Unit: milliseconds.
        clientConfig.setMaxRequestsPerHost(<maxRequestsPerHost>);// Optional. Specify the maximum number of requests per host.
        clientConfig.setMaxRequests(<maxRequests>);// Optional. Specify the maximum number of requests.
        clientConfig.setProtocolType(ProtocolType.HTTP); // Optional. Specify the request protocol. Default value: HTTP.
        /* Optional. Specify the IP address and port of the proxy.
        clientConfig.setHttpProxy("<http://192.168.XX.XX:33XX>");
        or
        clientConfig.setHttpsProxy("<https://192.168.XX.XX:33XX>");
        */
        profile.setHttpClientConfig(clientConfig);
        IAcsClient client = new DefaultAcsClient(profile);
        // Create an API request and specify parameters.
        DescribeNatGatewaysRequest request = new DescribeNatGatewaysRequest();
        // Service-related parameters.
        request.setPageSize(10);
        request.setPageNumber(1);
        // Specify the organization ID and resource set ID to query specified resources.
        request.putHeaderParameter("x-acs-organizationid", "1");
        request.putHeaderParameter("x-acs-resourcegroupid", "11");
        // Send the request and handle the response or exception.
        DescribeNatGatewaysResponse response;
       try {
            DescribeNatGatewaysResponse response = client.getAcsResponse(request);
            System.out.println(new Gson().toJson(response));
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            System.out.println("ErrCode:" + e.getErrCode());
            System.out.println("ErrMsg:" + e.getErrMsg());
            System.out.println("RequestId:" + e.getRequestId());
        }
     }
 }
```

3.2. Use SDK

3.2.1. Install VPC SDK for Java

This topic describes how to install and use Virtual Private Cloud (VPC) SDK for Java. To use the features of NAT Gateway, you must use VPC SDK.

Alibaba Cloud SDK for Java supports Java Development Kit (JDK) 1.8 or later. You can install Alibaba Cloud SDK for Java by adding Maven dependencies or downloading Alibaba Cloud SDK.

To use VPC SDK, you must install the core library of Alibaba Cloud SDK for Java and VPC SDK for Java. We recommend that you use the core library version 4.5.17 or later, and use VPC SDK for Java 3.2.0.

To use VPC SDK for Java, you must install the core library of Alibaba Cloud SDK for Java and add the following dependencies to the pom.xml file. For more information about the specific SDK version, see Alibaba Cloud SDK.

```
<dependencies>
        <dependency>
            <groupId>com.aliyun</groupId>
            <artifactId>aliyun-java-sdk-core</artifactId>
            <version>4.5.17</version>
        </dependency>
        <dependency>
            <groupId>com.aliyun</groupId>
            <artifactId>aliyun-java-sdk-vpc</artifactId>
            <version>3.2.0</version>
        </dependency>
</dependencies>
```

3.2.2. Configure authentication credentials

When you use Alibaba Cloud SDKs to access Apsara Stack services, you must provide an Apsara Stack tenant account for authentication. This topic describes how to configure authentication credentials.

SDK for Java supports authentication through an AccessKey pair. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

If you want to use your AccessKey pair to access Apsara Stack, you must specify the AccessKey pair when you initialize the client.

> **Note**
>
> Do not disclose any code that contains your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your account may be compromised.

```
DefaultProfile profile = DefaultProfile.getProfile(
    "<yourRegionID>",          // Replace it with your region ID.
    "<yourAccessKeyID>",      // Replace it with your AccessKey ID.
    "<yourAccessKeySecret>"); // Replace it with your AccessKey secret.
```

> **Note**
>
> Replace the preceding variables with your actual information. Remove the brackets (<>) when you specify the parameters.

3.2.3. Configure connection requests

This topic describes how to configure a connection request by using the HttpClientConfig object.

You can use the following code to configure the HttpClientConfig object. We recommend that you select and configure the following parameters based on your business requirements.

> **Note**
>
> You must use actual values to replace the variables in the following sample code. Do not retain the angle brackets (<>) in the final code.
>
> The following list describes the variables:
>
> - <readTimeout>: Specify the read timeout period based on your business requirements. Unit: milliseconds.
> - <connectionTimeout>: Specify the connection timeout period based on your business requirements. Unit: milliseconds.
> - <maxRequestsPerHost>: Specify the maximum number of requests that are supported by each server based on your business requirements. The supported data type is INTEGER.
> - <maxRequests>: Specify the maximum number of requests based on your business requirements. The supported data type is INTEGER.
> - <http://192.168.XX.XX:33XX>: Replace it with the actual IP address and port of the proxy.

```
// Obtain the HttpClientConfig object.
HttpClientConfig clientConfig = HttpClientConfig.getDefault();
// Specify whether to ignore certificates.
clientConfig.setIgnoreSSLCerts(true);
// (Optional) Specify the read timeout period. Unit: milliseconds.
clientConfig.setReadTimeoutMillis(<readTimeout>);
// (Optional) Specify the connection timeout period. Unit: milliseconds.
clientConfig.setConnectionTimeoutMillis(<connectionTimeout>);
// (Optional) Specify the maximum number of requests that are supported by each server. The supported data type is INTEGER.
clientConfig.setMaxRequestsPerHost(<maxRequestsPerHost>);
// (Optional) Specify the maximum number of requests. The supported data type is INTEGER.
clientConfig.setMaxRequests(<maxRequests>);
// (Optional) Specify the protocol type.
clientConfig.setProtocolType(ProtocolType.HTTP);
/** (Optional) Specify whether to configure the proxy based on your business requirements. The following code is available:
clientConfig.setHttpProxy("<http://192.168.XX.XX:33XX>");
Or
clientConfig.setHttpsProxy("<https://192.168.XX.XX:33XX>");
Replace https://192.168.XX.XX:33XX with the actual IP address and port of the proxy.
*/
profile.setHttpClientConfig(clientConfig);
```

3.2.4. Initiate a request

This topic describes how to use Virtual Private Cloud (VPC) SDK for Java to initiate a request. To use the features of NAT Gateway, you must use VPC SDK.

Procedure

1. Create an AcsClient.

   ```
   IAcsClient client = new DefaultAcsClient(profile);
   ```

2. Create a request.

   Name the request in the following format: `${apiName}Request`. Replace ${apiName} with an API operation name, for example, *DescribeNatGateways*.

   When multiple service SDKs are used, different requests may have the same name. You can differentiate the requests based on package names.

```
DescribeNatGatewaysRequest request = new DescribeNatGatewaysRequest();
// Service-related parameters.
request.setPageSize(10);
request.setPageNumber(1);
// Specify the organization ID and resource set ID to query specified resources.
request.putHeaderParameter("x-acs-organizationid", "1");
request.putHeaderParameter("x-acs-resourcegroupid", "");
```

3. Initiate the API request and handle the response or exceptions.

```
DescribeNatGatewaysResponse response;
try {
   DescribeNatGatewaysResponse response = client.getAcsResponse(request);
   System.out.println(new Gson().toJson(response));
} catch (ServerException e) {
    e.printStackTrace();
} catch (ClientException e) {
    e.printStackTrace();
}
```

All returned fields are deserialized in the response. You can call `response.getXXX()` to obtain the values of the response fields.

```
instanceStatus := response.getStatus()
```

However, if an exception occurs or you want to obtain the original HTTP response, use `doAction()` to obtain the original response.

```
HttpResponse response = client.doAction(request);
```

3.2.5. Troubleshooting

If the server or SDK encounters an error when you use SDK for Java, it returns an error response. The error response contains an error code and an error message.

In most cases, you do not need to handle the errors returned by SDK for Java. You need to only handle the errors returned by the server based on error messages.

- `ServerException` indicates a server error.
- `ClientException` indicates an SDK error.

For example, when the following error occurs, you can modify the AccessKey ID based on the error message to solve the problem:

```
com.aliyuncs.exceptions.ClientException: InvalidAccessKeyId.NotFound : Specified access key is not found.
```

If you want to handle SDK errors, refer to the following example to write your code:

```
try {
    FooResponse response = client.getAcsResponse(request);
    // Handle the response.
    // ...
}catch (ServerException e){
    // You can add your logic to handle errors.
    // For example, print the error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
    // If the error persists, you can submit a ticket with the request ID included.
    System.out.println("ResponseId=" + e.getRequestId());
}catch (ClientException e){
    // You can add your logic to handle errors.
    // For example, print the error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
}
```

3.2.6. Use CommonRequest to call API operations

If you want to call the API operations of a cloud service that does not provide SDKs, or you cannot use an SDK to call API operations whose requests and responses meet your business requirements, you can use CommonRequest to call API operations. You can use CommonRequest to call all API operations.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

- Light weight: You only need the core package to initiate the call, without downloading or installing the SDK of each product.
- Easy and convenient: You can call the latest API without updating the SDK.
- Fast iteration

Use CommonRequest to call an API operation

If you want to send a CommonRequest request, you must obtain the values of the following parameters. You can obtain the values of these parameters from the API references.

- Domain: the endpoint of the service.
- Version: the version of the API in the YYYY-MM-DD format.

  You can obtain the API version from the sections about common parameters in the API references.
- Action: the name of the API operation that you want to call.

  You need to obtain the value of the Action parameter and specify an API operation in `request.setSysAction("<Action>")`.

For example, if you want to call the DescribeNatGateways operation, you must use `request.setSysAction("DescribeNatGateways")` to specify the API operation when you initiate a CommonRequest request.

Example: Call an RPC API operation

The following sample code provides an example on how to call the `DescribeNatGateways` operation of NAT Gateway. The API operations of NAT Gateway use the RPC style.

> **Note** In the following code, replace the parameters with your actual information. Delete the angle brackets (<>) before you submit the code.
>
> The following section describes the parameters:
>
> - <yourRegionID>: Replace the parameter with the region ID.
> - <yourAccessKeyID>: Replace the parameter with your AccessKey ID.
> - <yourAccessKeySecret>: Replace the parameter with your AccessKey secret.
> - <yourSecurityToken>: Replace the parameter with your security token.
> - <yourResourceGroupID>: Replace the parameter with the resource set ID.
> - <yourOrganizationID>: Replace the parameter with the organization ID.
> - <yourInstanceID>: Replace the parameter with the instance ID.
> - <http://192.168.XX.XX:33XX>: Replace the parameter with the IP address and port of the proxy.

```
import com.aliyuncs.CommonRequest;
import com.aliyuncs.CommonResponse;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.http.HttpClientConfig;
import com.aliyuncs.http.ProtocolType;
public class Sample {
    public static void main(String[] args) {
        // Create a DefaultAcsClient instance and initialize the instance.
        DefaultProfile profile = DefaultProfile.getProfile(
            "<yourRegionUD>",          // Replace the parameter with the region ID.
            "<yourAccessKeyID>",      // Replace the parameter with your AccessKey ID.
            "<yourAccessKeySecret>"); // Replace the parameter with your AccessKey secret.
        HttpClientConfig clientConfig = HttpClientConfig.getDefault();
        clientConfig.setProtocolType(ProtocolType.HTTP);
        /**
        Optional. Configure the HTTP proxy based on your business requirements.
        Format:
        clientConfig.setHttpProxy("<http://192.168.XX.XX:33XX>");
        Specify the IP address and port of the proxy.
        */
        profile.setHttpClientConfig(clientConfig);
        IAcsClient client = new DefaultAcsClient(profile);
        // Create an API request and specify parameters.
        CommonRequest request = new CommonRequest();
        // Specify the endpoint of the service.
        request.setSysDomain("vpc.aliyuncs.com");
        request.setSysProduct("Vpc");
        request.setSysVersion("2016-04-28");
        request.setSysAction("DescribeNatGateways");
        request.putQueryParameter("PageNumber", "1");
        request.putQueryParameter("PageSize", "30");
        request.putHeadParameter("x-acs-resourcegroupid", "<yourResourceGroupID>");// Optional. Specify the resource set ID.
        request.putHeadParameter("x-acs-organizationid", "<yourOrganizationID>");// Required. Specify the organization ID.
        request.putHeadParameter("x-acs-regionid", "<yourRegionID>");// Optional. Specify the region ID. If you use Apsara Stack Enterprise V3.15.0 o
r earlier versions, this parameter is required.
        // request.putHeadParameter("x-acs-instanceid", "<yourInstanceID>");// Optional. Specify the instance ID. This parameter is required when you
want to delete, modify, or query an instance.
        /**
        When you use STS AccessKey credentials to call an API operation, you must add the SecurityToken field in the request parameters.
        Use the following method:
        request.putQueryParameter("SecurityToken", "<yourSecurityToken>");
        Specify your security token.
        */
        try {
            CommonResponse response = client.getCommonResponse(request);
            System.out.println(response.getData());
        } catch (ServerException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        } catch (ClientException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        }
    }
}
```

4.Call examples for SDK for Python

4.1. Quick start

This topic describes how to obtain and use Virtual Private Cloud (VPC) SDK for Python. To use the features of NAT Gateway, you must use VPC SDK.

Prerequisites

- An authorized account and an AccessKey pair (AccessKey ID and AccessKey secret) are obtained. For more information, see Obtain AccessKey credentials.
- The endpoint of NAT Gateway is obtained. For more information, see Obtain the endpoint of NAT Gateway.

Install VPC SDK for Python

1. Install the SDK core library.
   - If you use Python 2.x, run the following command to install the core library of Alibaba Cloud SDK:

     ```
     pip install aliyun-python-sdk-core
     ```

   - If you use Python 3.x, run the following command:

     ```
     pip3 install aliyun-python-sdk-core-v3
     ```

2. Install VPC SDK for Python.

   The following examples describe how to install VPC SDK for Python:

   - If you use Python 2.x, run the following command:

     ```
     pip install aliyun-python-sdk-vpc
     ```

   - If you use Python 3.x, run the following command:

     ```
     pip3 install aliyun-python-sdk-vpc
     ```

Use VPC SDK for Python

To use VPC SDK for Python, perform the following steps:

1. Create a client instance. When you create a client instance, you must obtain a region ID, AccessKey ID, and AccessKey secret.
2. Create an API request and specify the required parameters.
3. Initiate the API request and process the response or exception.

> **Note** In the following code, replace the parameters with your actual information. Delete the angle brackets (<>) before you submit the code.
>
> The following section describes the parameters:
>
> - <yourRegionID>: Replace the parameter with the region ID.
> - <yourAccessKeyID>: Replace the parameter with your AccessKey ID.
> - <yourAccessKeySecret>: Replace the parameter with your AccessKey secret.
> - <vpc.aliyuns.com>: Replace the parameter with the endpoint of the service.

```
#!/usr/bin/env python
#coding=utf-8
from aliyunsdkcore import client
from aliyunsdkcore.profile import region_provider
from aliyunsdkvpc.request.v20160428 import DescribeNatGatewaysRequest
# global config
region_id = '<yourRegionID>' # Specify the region ID.
access_key = '<yourAccessKeyID>' # Specify the AccessKey ID.
acces_secret = '<yourAccessKeySecret>' # Specify the AccessKey secret.
# product config
product_name = 'Vpc' # Specify the service name.
endpoint = '<vpc.aliyuns.com>' # Specify the endpoint of the service.
# create client
region_provider.modify_point(product_name, region_id, endpoint)
clt = client.AcsClient(access_key, acces_secret, region_id)
# setup request
request = DescribeNatGatewaysRequest.DescribeNatGatewaysRequest()
request.set_accept_format('json') # Specify the response format.
# get response
response = clt.do_action_with_exception(request)
print response # If you use Python 3.x, the code here is print (response).
```

4.2. Use SDK

4.2.1. Install SDK for Python

This topic describes how to install and use Virtual Private Cloud (VPC) SDK for Python. To use the features of NAT Gateway, you must use VPC SDK.

Alibaba Cloud SDK for Python supports Python 2.6.x, Python 2.7.x, and Python 3.x or later. You can install Alibaba Cloud SDK for Python by using pip.

> **Note** To use the SDK of a cloud service, you must install the core library of Alibaba Cloud SDK for Python. For example, if you want to use VPC SDK for Python, you must install the core library of Alibaba Cloud SDK for Python and VPC SDK for Python.

- If you use Python 2.x, run the following command:

```
pip install aliyun-python-sdk-core
```

- If you use Python 3.x, run the following command:

```
pip3 install aliyun-python-sdk-core-v3
```

The following example describes how to install VPC SDK.

- If you use Python 2.x, run the following command:

```
pip install aliyun-python-sdk-vpc
```

- If you use Python 3.x, run the following command:

```
pip3 install aliyun-python-sdk-vpc
```

4.2.2. Configure authentication credentials

When you use Alibaba Cloud SDK to access Apsara Stack services, you must provide an Apsara Stack tenant account for authentication.

SDK for Python supports authentication through an AccessKey pair. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

If you want to use your AccessKey pair to access Apsara Stack, you must specify the AccessKey pair when you initialize the client.

> **Notice** Do not disclose any code that contains your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your account may be compromised.

```
clt = client.AcsClient(secret_id, secret_key, region_id)
```

4.2.3. Handle errors

If an error occurs on the server side or SDK side when you use the Python SDK, the Python SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Generally, you are not required to handle the errors returned by the Python SDK. You are only required to handle the errors on the server side according to the error message.

- `ServerException` is the error message on the server side.
- `ClientException` is the error message on the SDK side.

For example, if the following error occurs, modify the ID of AccessKey according to the detailed error message.

```
aliyunsdkcore.acs\_exception.exceptions.ServerException: HTTP Status: 404 Error:InvalidAccessKeyId.NotFound Specified access key is not found.
```

To handle the errors returned by the Python SDK, see the following code example for reference:

```
try:
    response = client.do_action_with_exception(request)
except ServerException as e:
    # Add your own error handling logic here.
    # For example, print the detailed error message.
    print e.get_http_status()
    print e.get_error_code()
    print e.get_error_msg()
```

4.2.4. Set HTTPS requests

Apsara Stack SDK for Python allows you to initiate API requests over HTTP and HTTPS.

You can specify the HTTP or HTTPS protocol for a specific request, or set a global default protocol.

> **Note** The default HTTP or HTTPS protocol of a service takes precedence over the global default protocol.

Add OpenSSL support

The HTTPS protocol support of Apsara Stack SDK for Python is based on the OpenSSL support in Python. To use Apsara Stack SDK for Python to send HTTPS requests, you must add OpenSSL support in Python. OpenSSL supports TLS 1.2 and later.

Run the `python -c "import ssl"` command to check whether your Python environment supports OpenSSL. If the error message `ImportError: No module named ssl` is not returned, OpenSSL is already supported.

Otherwise, run the following command to install it:

```
pip install pyopenssl
```

Set the protocol to HTTP or HTTPS for a single request

The following sample code provides an example on how to set HTTPS as the protocol for a request:

```
request = DescribeInstancesRequest()
request.set_protocol_type("https")
# Set the value to https or http.
```

Set a global default protocol

The following sample code provides an example on how to set a global default protocol:

```
import aliyunsdkcore.request
aliyunsdkcore.request.set_default_protocol_type("https")
# Create a request and call client.do_action_with_exception() to send the request.
```

4.2.5. Initiate a request

This topic describes how to use VPC SDK for Python to initiate a request. To use the features of NAT Gateway, you must use VPC SDK.

Procedure

1. Import VPC SDK.

   ```
   from aliyunsdkcore import client
   from aliyunsdkcore.profile import region_provider
   from aliyunsdkvpc.request.v20160428 import DescribeNatGatewaysRequest
   ```

2. Create an AcsClient instance.

   ```
   client.region_provider.modify_point(product_name, region_id, endpoint)
   clt = client.AcsClient(access_key, access_secret, region_id)
   ```

3. Create a request object.

   ```
   request = DescribeNatGatewaysRequest.DescribeNatGatewaysRequest()
   request.set_accept_format('json')
   ```

4. Initiate the request and process the response.

   ```
   response = clt.do_action_with_exception(request)
   print response
   ```

4.2.6. Use CommonRequest to call API operations

If you want to call the API operations of a cloud service that does not provide SDKs, or you cannot use an SDK to call API operations whose requests and responses meet your business requirements, you can use CommonRequest to call API operations. You can use CommonRequest to call all API operations.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

- Light weight: You only need the core package to initiate the call, without downloading or installing the SDK of each product.
- Easy and convenient: You can call the latest API without updating the SDK.
- Fast iteration

Use CommonRequest to call an API operation

If you want to send a CommonRequest request, you must obtain the values of the following parameters: You can obtain the values of these parameters from the API references.

- Domain: specifies the service endpoint.
- Version: the version of the API in the YYYY-MM-DD format.

  You can obtain the API version from the sections about common parameters in the API references.
- Operation information: the name of the API operation that you want to call.

  To call an RPC API operation:

  You must obtain the value of the Action parameter and use `request.set_action_name('Action')` to specify the API operation.

  For example, if you want to call the DescribeNatGateways operation, you must use `request.set_action_name('DescribeNatGateways')` to specify the API operation when you initiate a CommonRequest request.

Example: Call an RPC API operation

The following sample code provides an example on how to call the `DescribeNatGateways` operation.

> **Note** In the following code, replace the parameters with actual values. Delete the angle brackets (<>) before you submit the code.
>
> The following section describes the parameters:
>
> - <yourRegionID>: Replace the parameter with the region ID.
> - <yourAccessKeyID>: Replace the parameter with your AccessKey ID.
> - <yourAccessKeySecret>: Replace the parameter with your AccessKey secret.
> - <yourSecurityToken>: Replace the parameter with your security token.
> - <yourResourceGroupID>: Replace the parameter with the resource set ID.
> - <yourOrganizationID>: Replace the parameter with the organization ID.
> - <yourInstanceID>: Replace the parameter with the instance ID.
> - <vpc.aliyuncs.com>: Replace the parameter with the endpoint of the service.

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.request import CommonRequest
# Specify the AccessKey ID, AccessKey secret, and region ID.
client = AcsClient('{<yourAccessKeyID>}', '{<yourAccessKeySecret>}', '{<yourRegionID>}')
request = CommonRequest()
request.set_product('Vpc')
request.set_action_name('DescribeNatGateways')
request.set_version('2016-04-28')
request.set_domain('<vpc.aliyuncs.com>') #Specify the endpoint of the service.
# or:
# request = = CommonRequest(product='Vpc', action_name='DescribeNatGateways',version='2016-04-28',domain='vpc.aliyuncs.com')
######
# Specify the request protocol. Valid values: https and http. Default value: http.
# You can specify HTTPS as the protocol in the following manner:
# request.set_protocol_type('https')
######
request.set_accept_format('json')
request.set_method('POST')
request.add_query_param('PageNumber', '1')
request.add_query_param('PageSize', '30')
######
# When you use an STS AccessKey 3-tuple to call an API operation, you must add the SecurityToken field in the request parameters.
# Format:
# request.add_query_param("SecurityToken", "<yourSecurityToken>");
# Specify your security token.
######
# Optional. Specify the resource set ID.
request.add_header("x-acs-resourcegroupid", "<yourResourceGroupID>")
# Required. Specify the organization ID.
request.add_header("x-acs-organizationid", "<yourOrganizationID>")
# Required. Specify the source of the API call.
request.add_header("x-acs-caller-sdk-source","ApiTestDemo")
# Optional. Specify the region ID. This parameter is required if you use Apsara Stack Enterprise V3.15.0 or earlier.
request.add_header("x-acs-regionid", "<yourRegionID>")
# Optional. Specify the instance ID. This parameter is required if you want to modify, delete, or query an instance.
# request.add_header("x-acs-instanceid", "<yourInstanceID>")
response = client.do_action_with_exception(request)
print(str(response, encoding = 'utf-8'))
```

5.Call examples for SDK for Go

5.1. Quick start

Alibaba Cloud SDK for Go allows you to access services without complex coding. This topic describes how to obtain and use Virtual Private Cloud (VPC) SDK for Go. To use the features of NAT Gateway, you must use VPC SDK.

Prerequisites

- An Apsara Stack tenant account and an AccessKey pair, which consists of an AccessKey ID and an AccessKey secret, are obtained. For more information, see Obtain AccessKey credentials.
- The endpoint of NAT Gateway is obtained. For more information, see Obtain the endpoint of NAT Gateway.

Install the core package of Alibaba Cloud SDK for Go

Alibaba Cloud SDK for Go supports Go 1.10.x and later. You can run the following command to install the core package: You can check whether the latest version of the core package is installed on the Alibaba Cloud SDK for Go page.

```
go get -u github.com/aliyun/alibaba-cloud-sdk-go/sdk
```

Use SDK for Go

To use SDK for Go, perform the following steps:

1. Initialize a client instance.
2. Create an API request and specify the required parameters.
3. Initiate the API request and process the response or exception.

> **Note** In the following code, replace the parameters with actual values. Delete the angle brackets (<>) before you submit the code.
>
> The following section describes the parameters:
>
> - <yourRegionID>: Replace the parameter with the region ID.
> - <yourAccessKeyID>: Replace the parameter with your AccessKey ID.
> - <yourAccessKeySecret>: Replace the parameter with your AccessKey secret.
> - <Endpoint>: Replace the parameter with the endpoint.

```
package main
import (
    "github.com/aliyun/alibaba-cloud-sdk-go/services/vpc"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "fmt"
)
func main() {
    // Create a vpcClient instance.
    vpcClient, err := vpc.NewClientWithAccessKey(
        "<yourRegionID>",             // Replace the parameter with the region ID.
        "<yourAccessKeyID>",         // Replace the parameter with your AccessKey ID.
        "<yourAccessKeySecret>")        // Replace the parameter with your AccessKey secret.
    if err != nil {
        // Handle exceptions.
        panic(err)
    }
    // Create a request and set the required parameters.
    request := vpc.CreateDescribeNatGatewaysRequest()
    // Specify the endpoint of the service.
    request.Domain = "<Endpoint>"
    // Set request.PageSize to 10.
    request.PageSize = requests.NewInteger(10)
    // Initiate the request and handle exceptions.
    response, err := vpcClient.DescribeNatGateways(request)
    if err != nil {
        // Handle exceptions.
        panic(err)
    }
    fmt.Println(response)
}
```

4. Optional. Switch to HTTP or HTTPS.

```
request.Scheme = "HTTPS"
```

5.2. Use SDK

5.2.1. Install the core package of SDK for Go

This topic describes how to install the core package of SDK for Go.

Apsara Stack SDK for Go supports Go 1.10.x and later. You can run the following command to install the core package:

```
go get -u github.com/aliyun/alibaba-cloud-sdk-go/sdk
```

5.2.2. Configure authentication credentials

When you use Alibaba Cloud SDK to access Apsara Stack services, you must provide an Apsara Stack tenant account for authentication.

SDK for Go supports authentication through an AccessKey pair. For more information, see Obtain AccessKey credentials.

If you want to use your AccessKey pair to access Apsara Stack, you must configure the AccessKey pair as the credentials when you initialize the client.

> **Notice** Do not disclose any code containing your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your account may be compromised.

The following code provides an example on how to initialize a vpcClient instance.

```
// Initialize a vpcClient instance.
vpcClient, err := vpc.NewClientWithAccessKey(
        "<yourRegionID>",               // Replace the parameter with the region ID.
        "<yourAccessKeyID>",            // Replace the parameter with your AccessKey ID.
        "<yourAccessKeySecret>")        // Replace the parameter with your AccessKey secret.
```

> **Note** In the preceding sample code, replace the parameters with the actual information. Delete the angle brackets (<>) before you submit the code.

5.2.3. Initiate a request

This topic describes how to use Virtual Private Cloud (VPC) SDK for Go to initiate a request. To use the features of NAT Gateway, you must use VPC SDK.

The following example shows how to use VPC SDK for Go to initiate a request.

1. Import VPC SDK for Go.

   ```
   import github.com/aliyun/alibaba-cloud-sdk-go/services/vpc
   ```

2. Create a VPC client. The client includes all APIs of the VPC.

   > **Note** In the following code, replace the parameters with your actual information. Delete the angle brackets (<>) before you submit the code.

   ```
   vpcClient,err := <vpc>.NewClientWithAccessKey(  //Replace the parameter with the name of the service.
       "<yourRegionID>",  // Replace the parameter with the region ID.
       "<yourAccessKeyID>",  // Replace the parameter with your AccessKey ID.
       "<yourAccessKeySecret>")  // Replace the parameter with your AccessKey secret.
   vpcClient.Domain = "vpc.aliyuns.com" //Specify the endpoint of the service.
   ```

3. Use the `xxx.CreateXXXRequest` method to create a request.

   The naming convention for this method is `${service}.Create${apiName}Request`.

   - ${service} specifies the service name in lowercase, such as *vpc*.
   - ${apiName} specifies the name of an API operation, such as *DescribeNatGateways*.

   ```
   request := vpc.CreateDescribeNatGatewaysRequest()
   request.InstanceId = ""
   ```

4. Send the request.

   ```
   response, err := vpcClient.DescribeNatGateways(request)
   ```

5.2.4. Handle errors

When you use Alibaba Cloud SDK for Go, a `ClientError` or a `ServerError` is returned when an error occurs on the server side or on the SDK side. Both error types are included in `sdk.errors`. The errors conform to the standard Go error interface, so they can be handled in a similar way as standard Go errors.

Handle errors

You can use the following code to handle errors:

```
response,err  := vpcClient.DescribeNatGateways(request)
if err != nil {
    // Obtain the error information.
   err.Error()
}
```

ClientError

When you send a request, if an error occurs in the SDK and cannot be automatically handled, the SDK returns a `ClientError`.

The following code shows how to determine and obtain information in a `ClientError`:

Notice When you use a specific error struct, you must add the error package `github.com/aliyun/alibaba-cloud-sdk-go/sdk/errors` by using the following code:

```
package main
import (
    "github.com/aliyun/alibaba-cloud-sdk-go/services/vpc" // Replace vpc with the name of the service.
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    // The error package that you want to add.
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/errors"
    "fmt"
)
```

```
response, err := vpcClient.DescribeNatGateways(request)
if clientError, ok := err.(*errors.ClientError); ok{
    // Obtain the error code.
    clientError.ErrorCode()
    // Obtain the error message.
    clientError.Message()
    // Obtain the original error. The return value may be nil.
    clientError.OriginError()
}
```

ServerError

When the server returns an error message, the SDK wraps the message into a `ServerError` and returns it to the client. In this case, you can still obtain the original HTTP response from the response.

The following code shows how to determine and obtain information in a ServerError and a response:

Notice When you use a specific error struct, you must add the error package `github.com/aliyun/alibaba-cloud-sdk-go/sdk/errors` by using the following code:

```
package main
import (
    "github.com/aliyun/alibaba-cloud-sdk-go/services/vpc" // Replace vpc with the name of the service.
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    // The error package that you want to add.
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/errors"
    "fmt"
)
```

```
response, err := vpcClient.DescribeNatGateways(request)
if serverError, ok := err.(*errors.ServerError); ok{
    // Obtain the error code.
    serverError.ErrorCode()
    // Obtain the error message.
    serverError.Message()
    // Obtain the original HTTP response.
    response.GetOriginHttpResponse()
}
```

5.2.5. Use CommonRequest to call API operations

If you want to call the API operations of a cloud service that does not provide SDKs, or you cannot use an SDK to call API operations whose requests and responses meet your business requirements, you can use CommonRequest to call API operations. You can use CommonRequest to call all API operations.

Example: Call an RPC API operation

The following sample code provides an example on how to call the `DescribeNatGateways` operation of NAT Gateway. The API operations of NAT Gateway use the RPC style.

Note In the following code, replace the parameters with actual values. Delete the angle brackets (<>) before you submit the code.

The following section describes the parameters:

- <yourRegionID>: Replace the parameter with the region ID.
- <yourAccessKeyID>: Replace the parameter with your AccessKey ID.
- <yourAccessKeySecret>: Replace the parameter with your AccessKey secret.
- <vpc.aliyuncs.com>: Replace the parameter with the endpoint of the service.
- <yourSecurityToken>: Replace the parameter with your security token.
- <yourResourceGroupID>: Replace the parameter with the resource set ID.
- <yourOrganizationID>: Replace the parameter with the organization ID.
- <yourInstanceID>: Replace the parameter with the instance ID.

```
package main
import (
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk"
    "fmt"
)
func main() {
    client, err := sdk.NewClientWithAccessKey(
        "<yourRegionID>",        //Replace the parameter with the region ID.
        "<yourAccessKeyID>",     //Replace the parameter with the AccessKey ID.
        "<yourAccessKeySecret>") //Replace the parameter with your AccessKey secret.
    if err != nil {
        panic(err)
    }
    request := requests.NewCommonRequest()
    request.Method = "POST"
    request.Domain = "<vpc.aliyuncs.com>" // Replace the parameter with the endpoint of the service.
    request.Product = "Vpc"
    request.Version = "2016-04-28"
    // This is an RPC API operation. Therefore, the ApiName(Action) parameter must be specified.
    request.ApiName = "DescribeNatGateways"
    // Configure service-related parameters.
    request.QueryParams["PageNumber"] = "1"
    request.QueryParams["PageSize"] = "30"
    /*
     When you use STS AccessKey credentials to call an RPC API operation, you must add the SecurityToken field in the request parameters.
     Format:
     request.QueryParams["SecurityToken"]="<yourSecurityToken>"
     Specify your security token.
     */
    request.Headers["x-acs-regionid"] = "<yourRegionID>" // Optional. Specify your region ID. This parameter is required if you use Apsara Stack Ente
rprise V3.15.0 or earlier.
    request.Headers["x-acs-resourcegroupid"] = "<yourResourceGroupID>" // Optional. Specify the resource set ID.
    request.Headers["x-acs-organizationid"] = "<yourOrganizationID>" // Required. Specify the organization ID.
    // request.Headers["x-acs-instanceid"] = "<yourInstanceID>" // Optional. Specify the instance ID. This parameter is required if you want to modif
y, delete, or query an instance.
    response, err := client.ProcessCommonRequest(request)
    if err != nil {
        panic(err)
    }
    fmt.Print(response.GetHttpContentString())
}
```

6.API reference

6.1. List of operations by function

The following table lists API operations available for use in NAT Gateway.

API	Description
CreateNatGateway	Creates a network address translation (NAT) gateway.
ModifyNatGatewayAttribute	Modifies the name and description of a NAT gateway.
ModifyNatGatewaySpec	Resizes a NAT gateway.
DeleteNatGateway	Deletes a specified NAT gateway.
DescribeNatGateways	Queries NAT gateways.
CreateForwardEntry	Adds DNAT entries to a DNAT table.
DeleteForwardEntry	Deletes a specified DNAT entry.
ModifyForwardEntry	Modifies a specified DNAT entry.
DescribeForwardTableEntries	Queries DNAT entries in a specified DNAT table.
CreateSnatEntry	Adds SNAT entries to an SNAT table.
DeleteSnatEntry	Deletes a specified SNAT entry.
ModifySnatEntry	Modifies a specified SNAT entry.
DescribeSnatTableEntries	Queries SNAT entries in a specified SNAT table.
CreateBandwidthPackage	Creates a NAT service plan.
ModifyBandwidthPackageSpec	Modifies the bandwidth of a NAT service plan.
DescribeBandwidthPackages	Queries NAT service plans in a specified region.
ModifyBandwidthPackageAttribute	Modifies the name and description of a specified NAT service plan.
DeleteBandwidthPackage	Deletes a specified NAT service plan.
AddBandwidthPackageIps	Adds public IP addresses to a NAT service plan.
RemoveBandwidthPackageIps	Removes a public IP address from a NAT service plan.

6.2. Make API requests

6.2.1. Request structure

To send a NAT Gateway API request, you must send an HTTP GET request to the NAT Gateway endpoint. Before you send a request, you must specify the request parameters for the operation. A response is returned for each request. Requests and responses are encoded in UTF-8.

NAT Gateway API operations use the RPC protocol. You can call NAT Gateway API operations by sending HTTP GET requests.

The following request syntax is used:

```
http://Endpoint/?Action=xx&Parameters
```

where:

- Endpoint: the endpoint of the NAT Gateway API. The endpoint of the NAT Gateway API is `vpc.example.com`.

  > **Note** `example.com` is a custom domain name. For information about how to obtain a service endpoint, see Obtain the endpoint of ASAPI.

- Action: the name of the operation that you want to perform. For example, to query NAT gateways, you must set the Action parameter to DescribeNatGateways.
- Version: the version of the API that you want to call. The current NAT Gateway API version is *2016-04-28*.
- Parameters: the request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common parameters include the API version and authentication information. For more information about common parameters, see Common parameters.

The following example demonstrates how to call the DescribeNatGateways operation to query NAT gateways:

> **Note** The following code is formatted for ease of reading.

```
https://vpc.example.com/?Action=DescribeNatGateways
&Format=xml
&Version=2016-04-28
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
```

6.2.2. API authorization

To ensure the security of your account, we recommend that you call NAT Gateway API operations as a RAM user. To call NAT Gateway API operations as a RAM user, you must create and attach authorization policies to the RAM user.

For more information about the NAT Gateway resources and API operations that allow the authorization, see RAM authentication.

6.2.3. Signature

You must sign all API requests to ensure security. Apsara Stack uses the request signature to verify the identity of the API caller.

NAT Gateway implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair is an identity credential issued to Apsara Stack accounts and RAM users that is similar to a logon username and password. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of the user, while the AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential. For more information about how to create an AccessKey pair, see Obtain AccessKey credentials.

You must add the signature to an RPC API request in the following format:

`https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=xxxx%xxxx%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf`

Take DescribeNatGateways as an example. Assume that the AccessKey ID is `testid` and the AccessKey secret is `testsecret`, the following code shows the original request URL:

```
http://vpc.example.com/?Action=DescribeNatGateways
&Timestamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2016-04-28
&SignatureVersion=1.0
```

Perform the following operations to calculate the signature:

1. Use the request parameters to create a string-to-sign.

   ```
   GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeNatGateways&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad
   82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2014-05-15
   ```

2. Calculate the HMAC value of the string-to-sign.

   Append an ampersand (&) to the end of the AccessKey secret as the key to calculate the HMAC value. In this example, the key is `testsecret&`.

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. Add the signature string to the request:

   ```
   http://vpc.example.com/?Action=DescribeNatGateways
   &Timestamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2016-04-28
   &SignatureVersion=1.0
   &Signature=xxxx%xxxx%3D
   ```

6.3. RAM authentication

Before you call a NAT Gateway operation as a RAM user, you must use an Apsara Stack tenant account to create an authorization policy to grant permissions to the RAM user. In the authorization policy, an Alibaba Cloud Resource Name (ARN) is used to specify a resource.

NAT Gateway resources that allow authorized access

The following table lists the NAT Gateway resources that allow authorized access and their ARNs.

Resource type	ARN
NAT gateways	`acs:vpc:$regionid:$accountid:natgateway/$natgatewayid`
	`acs:vpc:$regionid:$accountid:natgateway/*`
	`acs:vpc*:$accountid:vpc/*`
	`acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid`

Resource type	ARN
NAT bandwidth packages	acs:vpc:$regionid:$accountid:bandwidthpackage/*
	aacs:vpc:*:$accountid:vpc/*
Forwarding tables	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
	acs:vpc:$regionid:$accountid:forwardtable/*
	acs:vpc:*:$accountid:vpc/*
SNAT tables	acs:vpc:$regionid:$accountid:snattable/$snattableid
	acs:vpc:$regionid:$accountid:snattable/*
	acs:vpc:*:$accountid:vpc/*
General resources	acs:vpc:$regionid:$accountid:*
	acs:vpc:*:$accountid:*

$regionid/*accoutid*/*vrouterid* are IDs of the specific resources, * represents all resources.

NAT Gateway API operations that allow authorized access

The following table lists the NAT Gateway API operations that allow authorized access and their ARNs.

Operation	ARN
CreateNatGateway	acs:vpc:$regionid:$accountid:natgateway/*
DescribeNatGateways	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid
	acs:vpc:$regionid:$accountid:natgateway/*
ModifyNatGatewaySpec	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid
ModifyNatGatewayAttribute	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid
	acs:ecs:$regionid:$accountid:instance/$instanceid
DeleteNatGateway	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid
	acs:ecs:$regionid:$accountid:instance/$instanceid
CreateBandwidthPackage	acs:vpc:$regionid:$accountid:bandwidthpackage/*
DescribeBandwidthPackages	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
	acs:vpc:$regionid:$accountid:bandwidthpackage/*
ModifyBandwidthPackageSpec	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
ModifyBandwidthPackageAttribute	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
AddBandwidthPackageIps	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
RemoveBandwidthPackageIps	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
DeleteBandwidthPackage	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
CreateForwardEntry	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
DeleteForwardEntry	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
ModifyForwardEntry	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
DescribeForwardTableEntries	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
CreateSnatEntry	acs:vpc:$regionid:$accountid:snattable/*
ModifySnatEntry	acs:vpc:$regionid:$accountid:snattable/$snattableid
DescribeSnatTableEntries	acs:vpc:$regionid:$accountid:snattable/$snattableid
DeleteSnatEntry	acs:vpc:$regionid:$accountid:snattable/$snattableid

6.4. Common parameters

This topic describes common parameters, including common request parameters and common response parameters. Common parameters are required in all API operations, regardless of the operation being called.

Common request parameters

Common request parameters must be included in all EIP API requests.

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The format in which to return the response. Valid values: *JSON and XML. Default value: JSON.*
Version	String	Yes	The version number of the API. Format: `YYYY-MM-DD`. Set the value to *2016-04-28*
AccessKeyId	String	Yes	The AccessKey ID provided to you by Apsara Stack.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to *HMAC-SHA1*
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time must be in UTC. For example, 2013-01-10T12:00:00Z.
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.

Examples

```
http://vpc.example.com/?Action=DescribeEipAddresses
&Timestamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2016-04-28
&SignatureVersion=1.0
```

Common response parameters

API responses use the HTTP response format where a 2XX status code indicates a successful call and a 4XX or 5XX status code indicates a failed call. Responses can be returned in either the JSON or XML format. You can specify the response format in the request. The default response format is XML.

Every response returns a unique RequestId regardless of whether the call is successful.

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
      <!—Result Root Node-->
      <Interface Name+Response>
      <!—Return Request Tag-->
      <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
      <!—Return Result Data-->
      </Interface Name+Response>
```

- JSON format

```
{
      "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
      /*Return Result Data*/
  }
```

6.5. NAT gateways

6.5.1. CreateNatGateway

Creates a NAT gateway.

Descriptions

When you call this operation, take note of the following items:

- You cannot deploy a NAT gateway and a user-created SNAT gateway in the same virtual private cloud (VPC) if the SNAT gateway is an Elastic Compute Service (ECS) instance.
- After a NAT gateway is created, a route entry is automatically added to the route table of the VPC. The destination CIDR block of the route entry is 0.0.0.0/0 and the next hop of the route entry is the NAT gateway. The route entry ensures that traffic is routed to the NAT gateway.
- If the route table of the VPC already contains a route entry whose destination CIDR block is 0.0.0.0/0, delete the route entry. Otherwise, you cannot create a NAT gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateNatGateway	The operation that you want to perform. Set the value to **CreateNatGateway**.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed. You can call the `DescribeRegions` operation to query the most recent region list.
VpcId	String	Yes	vpc-bp1di7uewzmtvfuq8****	The ID of the VPC.
Name	String	No	fortest	The name of the NAT gateway. The name must be 2 to 128 characters in length and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter and cannot start with `http://` or `https://`. If you do not specify this parameter, the ID of the NAT gateway is used by default.
Description	String	No	testnat	The description of the NAT gateway. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
ClientToken	String	No	shefffxxddjehfh****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.
Spec	String	No	Small	The size of the NAT gateway. Valid values: • **Small**(default): small • **Middle**: middle • **Large**: large • **XLarge.1**: super large
BandwidthPackage.N.IpCount	Integer	No	5	The number of public IP addresses in the NAT service plan. Valid values: **1** to **50**. N indicates the sequence number of the NAT service plan. Valid values: **1** to **4**.
BandwidthPackage.N.Bandwidth	Integer	No	5	The bandwidth limit of NAT service plan N. Unit: Mbit/s. Valid values: **5** to **5000**.
BandwidthPackage.N.Zone	String	No	cn-neimeng-env133-d01	The zone of NAT service plan N. If you do not set this parameter, the service plan is randomly allocated to a zone. Even if the IP addresses of the NAT service plan and the backend ECS instances belong to different zones, the ECS instances can still connect to the NAT gateway. However, you can reduce the network latency by allocating the NAT service plan to the zone where your ECS instances are deployed.
BandwidthPackage.N.ISP	String	No	BGP	By default, the type of Internet Service Provider (ISP) line of NAT service plan N is **BGP** (Multi-ISP).
BandwidthPackage.N.InternetChargeType	String	No	95	Specifies the billing method of the NAT service plan.
InstanceChargeType	String	No	PostPaid	The billing method. Valid values: • **PrePaid**: subscription • **PostPaid** (default): pay-as-you-go
PricingCycle	String	No	Month	The billing cycle of a subscription NAT service plan. Valid values: • **Month** (default): The NAT service plan is billed on a monthly basis. • **Year**: The NAT service plan is billed on an annual basis. This parameter is required if **InstanceChargeType** is set to **PrePaid**. This parameter is optional if **InstanceChargeType** is set to **PostPaid**.

Parameter	Type	Required	Example	Description
Duration	String	No	1	The subscription duration. • If **PricingCycle** is set to **Month**, set **Period** to a value from **1 to 9**. • If **PricingCycle** is set to **Year**, set **Period** to a value from **1 to 3**. • This parameter is required when **InstanceChargeType** is set to **PrePaid**.
AutoPay	Boolean	No	false	Specifies whether to enable automatic payment. Valid values: • **false**: disables automatic payment. After an order is generated, you must go to the Order Center to make the payment. • **true**: enables automatic payment. Payments are automatically made. This parameter is required when **InstanceChargeType** is set to **PrePaid**. This parameter is optional when **InstanceChargeType** is set to **PostPaid**.
VSwitchId	String	No	vsw-n2yf2tj1k2bfey5pq****	The ID of the vSwitch.
NatType	String	No	Normal	The type of the NAT gateway.
InternetChargeType	String	No	PayByLcu	The metering method of the NAT gateway.

Response parameters

Parameter	Type	Example	Description
NatGatewayId	String	ngw-112za33e4****	The ID of the NAT gateway. The ID is a unique identifier that is automatically generated by the system.
ForwardTableIds	List	ftb-11tc6xgmv****	The list of DNAT entries.
BandwidthPackageIds	List	bwp-11odxu2k7****	The list of NAT service plans.
RequestId	String	2315DEB7-5E92-423A-91F7-4C1EC9AD97C3	The ID of the request.
SnatTableIds	List	stb-SnatTableIds****	The list of SNAT entries.

Examples

Sample requests

```
https://vpc.aliyuncs.com/?Action=CreateNatGateway
&RegionId=cn-hangzhou
&VpcId= vpc-bp1di7uewzmtvfuq8****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CreateNatGatewayResponse>
    <BandwidthPackageIds>
  </BandwidthPackageIds>
    <RequestId>7C01CA72-73FD-4056-B16A-42E392D47625</RequestId>
    <SnatTableIds>
          <SnatTableId>stb-wz9aq9mec6f843j45****</SnatTableId>
    </SnatTableIds>
    <ForwardTableIds>
          <ForwardTableId>ftb-wz9sl3znmxhy605f8****</ForwardTableId>
    </ForwardTableIds>
    <NatGatewayId>ngw-wz95lh0c2wj9b6r1z****</NatGatewayId>
</CreateNatGatewayResponse>
```

`JSON` format

```
{
    "BandwidthPackageIds": {
        "BandwidthPackageId": []
    },
    "RequestId": "7C01CA72-73FD-4056-B16A-42E392D47625",
    "SnatTableIds": {
        "SnatTableId": [
            "stb-wz9aq9mec6f843j45****"
        ]
    },
    "ForwardTableIds": {
        "ForwardTableId": [
            "ftb-wz9sl3znmxhy605f8****"
        ]
    },
    "NatGatewayId": "ngw-wz95lh0c2wj9b6r1z****"
}
```


Error codes

HttpCode	Error code	Error message	Description
400	InvalidVPCStatus	vpc incorrect status.	The error message returned because the operation is not supported when the VPC is in the current state. Check whether the status of the VPC is valid.
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
400	InvalidNatGatewayName.Malformed	NatGateway name is not valid.	The error message returned because the specified gateway name is invalid.
400	InvalidNatGatewayDescription.MalFormed	NatGateway description is not valid.	The error message returned because the description of the specified gateway is invalid.
400	MissingParameter.BandwidthPackage	only support one BandwidthPackage be created with NatGateway.	The error message returned because no NAT service plan is specified.
404	InvalidVpcId.NotFound	Specified value of VpcId is not found in our record.	The error message returned because the specified VPC does not exist. Check whether the specified VPC is valid.
400	MissingParameter	Miss mandatory parameter.	The error message returned because the required parameters are not set. Check whether you have set all the required parameters before you call this operation.
404	InvalidZoneId.NotFound	Specified value of ZoneId is not exists.	The error message returned because the specified zone does not exist.
404	InvalidZoneId.NotFound	Can not find ZoneId for allocated ip.	The error message returned because the zone of the specified IP address is invalid.
400	QuotaExceeded.BandwidthPackageIps	The specified ipCount exceeded quota.	The error message returned because the number of IP addresses has reached the upper limit. Go to the Quota Management page and request a quota increase.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name is invalid. Enter the name in the correct format.
400	InvalidParameter.Description.Malformed	The specified Description is not valid.	The error message returned because the specified description is invalid.
400	ZONE_NO_AVAILABLE_IP	The Zone have no available ip.	The error message returned because no IP addresses are available in the zone.
400	InvalidParameter.BandwidthPackage.n.ISP.ValueNotSupport	The specified ISP of BandwidthPackage is not valid.	The error message returned because the specified ISP of the NAT service plan is invalid.
400	InvalidNatGatewayId.NotFound	The NatGatewayId not exist.	The error message returned because the specified NAT gateway ID does not exist. Check whether the NAT gateway ID is valid.
400	VswitchStatusError	The VSwitch is creating .	The error message returned because the operation is not supported when the system is creating the vSwitch.
400	VpcStatusError	The Vpc is creating .	The error message returned because the operation is not supported when the system is creating the VPC.
400	InvalidParameter.Spec.ValueNotSupported	The specified Spec is not valid.	The error message returned because the specified gateway size is invalid.
400	Forbidden.CheckEntryRuleQuota	Route entry quota rule check error.	The error message returned because an error occurs when the system checks the quota of route entries.

6.5.2. ModifyNatGatewayAttribute

Modifies the name and description of a NAT gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyNatGatewayAttribute	The operation that you want to perform. Set the value to **ModifyNatGatewayAttribute**.
NatGatewayId	String	Yes	ngw-2ze0dcn4mq31qx2jc****	The ID of the NAT gateway that you want to modify.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed. You can call the `DescribeRegions` operation to query the most recent region list.
Name	String	No	nat123	The name of the NAT gateway that you want to modify. The name must be 2 to 128 characters in length and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter. The name cannot start with `http://` or `https://`. **Note** You must specify at least one of the following parameters: **Name** and **Description**.
Description	String	No	fortest	The description of the NAT gateway. The description must be 2 to 256 characters in length, and must start with a letter. It cannot start with `http://` or `https://`. **Note** You must specify at least one of the following parameters: **Name** and **Description**.

Response parameters

Parameter	Type	Example	Description
RequestId	String	AB5F62CF-2B60-4458-A756-42C9DFE108D1	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyNatGatewayAttribute
&NatGatewayId=ngw-2ze0dcn4mq31qx2jc****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyNatGatewayAttributeResponse>
  <RequestId>AB5F62CF-2B60-4458-A756-42C9DFE108D1</RequestId>
</ModifyNatGatewayAttributeResponse>
```

`JSON` format

```
{"RequestId":"AB5F62CF-2B60-4458-A756-42C9DFE108D1"}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidNatGatewayId.NotFound	The specified NatGatewayId does not exist in our records.	The error message returned because the specified NAT gateway ID does not exist. Check whether the NAT gateway ID is valid.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name is invalid.

HttpCode	Error code	Error message	Description
400	InvalidParameter.Description.Malformed	The specified Description is not valid.	The error message returned because the specified description is invalid.

6.5.3. ModifyNatGatewaySpec

Resizes a NAT gateway.

Description

NAT gateways are available in different sizes. The size of a NAT gateway determines the Source Network Address Translation (SNAT) performance of the gateway, such as the maximum number of connections and the number of new connections per second. However, the data throughput is not affected.

The following table describes the correlations between different sizes of NAT gateways and SNAT performance metrics.

Size	Maximum connection	Number of new connections per second
Small	10,000	1,000
Medium	50,000	5,000
Large	200,000	10,000

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyNatGatewaySpec	The operation that you want to perform. Set the value to **ModifyNatGatewaySpec**.
NatGatewayId	String	Yes	ngw-bp1uewa15k4iy5770****	The ID of the NAT gateway.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed.
Spec	String	Yes	Small	The size of the NAT gateway. Valid values: • **Small**: a small-sized NAT gateway • **Middle**: a middle-sized NAT gateway • **Large**: a large-sized NAT gateway
AutoPay	Boolean	No	false	Specifies whether to enable automatic payment. Valid values: • **true**: enables automatic payment. • **false**: disables automatic payment. This is the default value.
ClientToken	String	No	SHA234js121223****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Example	Description
RequestId	String	DBD4E4A2-786E-4BD2-8EB6-107FFC2B5B7D	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyNatGatewaySpec
&NatGatewayId=ngw-bp1uewa15k4iy5770****
&RegionId=cn-qingdao-env17-d01
&Spec=Small
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyNatGatewaySpecResponse>
      <RequestId>DBD4E4A2-786E-4BD2-8EB6-107FFC2B5B7D</RequestId>
</ModifyNatGatewaySpecResponse>
```

`JSON` format

```
{
    "RequestId":"DBD4E4A2-786E-4BD2-8EB6-107FFC2B5B7D"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidNatGatewayId.NotFound	The specified NatGatewayId does not exist in our records.	The error message returned because the specified NAT gateway ID does not exist. Check whether the NAT gateway ID is valid.
400	NATGW_MODIFY_SPEC_SAME	The specified Spec is same with now.	The error message returned because the specified gateway size is the same as the current one.
400	InvalidParameter.Spec.ValueNotSupported	The specified Spec is not valid.	The error message returned because the specified gateway size is invalid.

6.5.4. DeleteNatGateway

Deletes a specified NAT gateway.

> **Note** Before you delete a NAT gateway, you must disassociate NAT service plans from the NAT gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteNatGateway	The operation that you want to perform. Set the value to **DeleteNatGateway**.
NatGatewayId	String	Yes	ngw-bp1uewa15k4iy5770****	The ID of the NAT gateway.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed. You can call the `DescribeRegions` operation to query the most recent region list.
Force	Boolean	No	false	Specifies whether to forcibly delete the NAT gateway. Valid values: • **true**: forcibly deletes the NAT gateway. • **false**: does not forcibly delete the NAT gateway.

Response parameters

Parameter	Type	Example	Description
RequestId	String	4EC47282-1B74-4534-BD0E-403F3EE64CAF	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteNatGateway
&NatGatewayId=ngw-bp1uewa15k4iy5770****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DeleteNatGatewayResponse>
  <RequestId>4EC47282-1B74-4534-BD0E-403F3EE64CAF</RequestId>
</DeleteNatGatewayResponse>
```

`JSON` format

```
{
    "RequestId": "4EC47282-1B74-4534-BD0E-403F3EE64CAF"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidNatGatewayId.NotFound	The specified NatGatewayId does not exist in our records.	The error message returned because the specified NAT gateway ID does not exist. Check whether the NAT gateway ID is valid.
400	DependencyViolation.BandwidthPackages	There are BandwidthPackages on specified NatGateway not deleted.	The error message returned because one or more NAT service plans are associated with the NAT gateway. Disassociate all NAT service plans from the NAT gateway and try again.

6.5.5. DescribeNatGateways

Queries NAT gateways.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeNatGateways	The operation that you want to perform. Set the value to **DescribeNatGateways**.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateways are deployed. You can call the `DescribeRegions` operation to query the most recent region list.
NatGatewayId	String	No	ngw-bp1uewa15k4iy5770****	The ID of the NAT gateway.
VpcId	String	No	vpc-bp15zckdt37pq72z****	The ID of the virtual private cloud (VPC).
Name	String	No	test	The name of the NAT gateway.
InstanceChargeType	String	No	PostPaid	The billing method of the NAT gateway. Valid values: • **PostPaid**: pay-as-you-go • **PrePaid**: subscription
Spec	String	No	Large	The size of the NAT gateway. Valid values: • **Small**: small • **Middle**: middle • **Large**: large • **XLarge.1**: super large
NatType	String	No	Normal	The type of the NAT gateway. Set the value to **Normal**, which specifies a standard NAT gateway.
ResourceGroupId	String	No	rg-bp67acfmxazb4ph****	The ID of the resource group to which the NAT gateway belongs.
PageNumber	Integer	No	10	The number of the page to return.
PageSize	Integer	No	1	The number of entries to return on each page.
DryRun	Boolean	No	true	Specifies whether to precheck the request only. Valid values: **true**: prechecks the request only. Resources are not queried. The system checks whether the AccessKey pair is valid, whether the Resource Access Management (RAM) user is authorized, and whether the required parameters are specified. If the request fails the precheck, the corresponding error message is returned. If the request passes the precheck, the `DryRunOperation` error code is returned. **false**: prechecks the request. This is the default value. After the request passes the precheck, a 2xx HTTP status code is returned and resources are queried.

Response parameters

Parameter	Type	Example	Description
NatGateways	Array of NatGateway		Detailed information about the NAT gateway.
NatGateway			
AutoPay	Boolean	true	Indicates whether automatic payment is enabled. Valid values: • **false**: automatic payment is disabled. After an order is generated, you must go to the Order Center to make the payment. • **true**: automatic payment is enabled. Payments are automatically made.
BandwidthPackageIds	List	bwp-s6lmotmkk****	The ID of the service plan associated with the NAT gateway.
BusinessStatus	String	Normal	The status of the NAT gateway. Valid values: • **Normal**: The NAT gateway works as expected. • **FinancialLocked**: The NAT gateway is locked due to overdue payments. • **SecurityLocked**: The NAT gateway is locked due to security reasons.
CreationTime	String	2017-06-08T12:20:55	The time when the NAT gateway was created. The time follows the ISO 8601 standard in the YYYY-MM-DDThh:mm:ssZ format. The time is displayed in UTC.
DeletionProtection	Boolean	true	Indicates whether deletion protection is enabled. Valid values: • **true**: enabled • **false**: disabled
Description	String	NAT	The description of the NAT gateway.
EcsMetricEnabled	Boolean	true	Indicates whether the traffic monitoring feature is enabled. Valid values: • **true**: enabled • **false**: disabled
ExpiredTime	String	2017-08-26T16:00Z	The time when the NAT gateway expires.
ForwardTableIds	List	ftb-uf6gj3mhsg94qsqst****	The list of DNAT entries.
InstanceChargeType	String	PostPaid	The billing method of the NAT gateway. Valid values: • **PostPaid**: pay-as-you-go • **PrePaid**: subscription
InternetChargeType	String	PayBySpec	The metering method of the NAT gateway. Only **PayBySpec** is returned, which indicates the pay-by-specification metering method.
IpLists	Array of IpList		Detailed information about the elastic IP address (EIP) that is associated with the NAT gateway.
IpList			
AllocationId	String	eip-n2y6nbm9z7t1l3xfz****	The ID of the EIP that is associated with the NAT gateway.
ApAccessEnabled	Boolean	false	Indicates whether access points are configured. Valid values: • **true**: access points are configured. • **false**: access points are not configured.
IpAddress	String	116.62.XX.XX	The EIP.
SnatEntryEnabled	Boolean	false	Indicates whether the EIP is specified in an SNAT entry.
UsingStatus	String	UsedBySnatTable	The status of the EIP.
Name	String	abc	The name of the NAT gateway.

Parameter	Type	Example	Description
NatGatewayId	String	ngw-bp1047e2d4z7kf2ki****	The ID of the NAT gateway.
NatGatewayPrivateInfo	Struct		Private information about the NAT gateway. If **NatType** is set to **Normal**, all parameters returned in this list are empty.
EniInstanceId	String	10	The instance ID of the elastic network interface (ENI).
IzNo	String	cn-hangzhou-b	The zone ID of the instance.
MaxBandwidth	Integer	5120	The bandwidth limit. Unit: Mbit/s.
PrivateIpAddress	String	192.168.1.xx	The private IP address.
VswitchId	String	vsw-bp1s2laxhdf9ayjbo****	The ID of the vSwitch.
NatType	String	Normal	The type of the NAT gateway.
RegionId	String	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed.
ResourceGroupId	String	rg-bp67acfmxazb4ph****	The ID of the resource group to which the NAT gateway belongs.
SnatTableIds	List	stb-uf6dalcdu0krz423p****	The list of SNAT entries of the NAT gateway.
Spec	String	Small	The size of the NAT gateway.
Status	String	Initiating	The status of the NAT gateway. Valid values: • **Initiating**: The NAT gateway is being initialized. • **Available**: The NAT gateway is available. • **Pending**: The NAT gateway is being configured.
VpcId	String	vpc-bp15zckdt37pq72z****	The ID of the VPC.
PageNumber	Integer	10	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	4EC47282-1B74-4534-BD0E-403F3EE64CAF	The ID of the request.
TotalCount	Integer	10	The total number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeNatGateways
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeNatGatewaysResponse>
  <TotalCount>10</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>4EC47282-1B74-4534-BD0E-403F3EE64CAF    </RequestId>
  <PageNumber>10</PageNumber>
  <NatGateways>
        <Status>Initiating</Status>
        <Description>NAT</Description>
        <ResourceGroupId>rg-bp67acfmxazb4ph****</ResourceGroupId>
        <InstanceChargeType>PostPaid</InstanceChargeType>
        <DeletionProtection>true</DeletionProtection>
        <AutoPay>true</AutoPay>
        <NatType>Normal</NatType>
        <BusinessStatus>Normal</BusinessStatus>
        <InternetChargeType>PayBySpec</InternetChargeType>
        <Name>abc</Name>
        <EcsMetricEnabled>true</EcsMetricEnabled>
        <VpcId>vpc-bp15zckdt37pq72z****</VpcId>
        <ExpiredTime>2017-08-26T16:00Z</ExpiredTime>
        <CreationTime>2017-06-08T12:20:55</CreationTime>
        <RegionId>cn-qingdao-env17-d01</RegionId>
        <Spec>Small</Spec>
        <NatGatewayId>ngw-bp1047e2d4z7kf2ki****</NatGatewayId>
        <IpLists>
              <UsingStatus>UsedBySnatTable</UsingStatus>
              <ApAccessEnabled>false</ApAccessEnabled>
              <SnatEntryEnabled>false</SnatEntryEnabled>
              <AllocationId>eip-n2y6nbm9z7t1l3xfz****</AllocationId>
              <IpAddress>116.62.XX.XX</IpAddress>
        </IpLists>
        <ForwardTableIds>ftb-uf6gj3mhsg94qsqst****</ForwardTableIds>
        <SnatTableIds>stb-uf6dalcdu0krz423p****</SnatTableIds>
        <BandwidthPackageIds>bwp-s61motmkk****</BandwidthPackageIds>
        <NatGatewayPrivateInfo>
              <IzNo>cn-hangzhou-b</IzNo>
              <PrivateIpAddress>192.168.1.xx</PrivateIpAddress>
              <MaxBandwidth>5120</MaxBandwidth>
              <EniInstanceId>10</EniInstanceId>
              <VswitchId>vsw-bp1s2laxhdf9ayjbo****</VswitchId>
        </NatGatewayPrivateInfo>
  </NatGateways>
</DescribeNatGatewaysResponse>
```

`JSON` format

```
{
    "TotalCount": 10,
    "PageSize": 10,
    "RequestId": "4EC47282-1B74-4534-BD0E-403F3EE64CAF",
    "PageNumber": 10,
    "NatGateways": {
        "Status": "Initiating",
        "Description": "NAT",
        "ResourceGroupId": "rg-bp67acfmxazb4ph****",
        "InstanceChargeType": "PostPaid",
        "DeletionProtection": true,
        "AutoPay": true,
        "NatType": "Normal",
        "BusinessStatus": "Normal",
        "InternetChargeType": "PayBySpec",
        "Name": "abc",
        "EcsMetricEnabled": true,
        "VpcId": "vpc-bp15zckdt37pq72z****",
        "ExpiredTime": "2017-08-26T16:00Z",
        "CreationTime": "2017-06-08T12:20:55",
        "RegionId": "cn-qingdao-env17-d01",
        "Spec": "Small",
        "NatGatewayId": "ngw-bp1047e2d4z7kf2ki****",
        "IpLists": {
            "UsingStatus": "UsedBySnatTable",
            "ApAccessEnabled": false,
            "SnatEntryEnabled": false,
            "AllocationId": "eip-n2y6nbm9z7t113xfz****",
            "IpAddress": "116.62.XX.XX"
        },
        "ForwardTableIds": "ftb-uf6gj3mhsg94qsqst****",
        "SnatTableIds": "stb-uf6dalcdu0krz423p****",
        "BandwidthPackageIds": "bwp-s6lmotmkk****",
        "NatGatewayPrivateInfo": {
            "IzNo": "cn-hangzhou-b",
            "PrivateIpAddress": "192.168.1.xx",
            "MaxBandwidth": 5120,
            "EniInstanceId": 10,
            "VswitchId": "vsw-bp1s2laxhdf9ayjbo****"
        }
    }
}
```


Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.

6.6. DNAT tables

6.6.1. CreateForwardEntry

Adds a DNAT entry to a DNAT table.

Description

Each DNAT entry consists of the following parameters: ExternalIp, ExternalPort, Protocol, InternalIp, and InternalPort. After you add a DNAT entry, the NAT gateway forwards packets of the specified protocol from [ExternalIp: ExternalPort] to [InternalIp: InternalPort] and sends responses back over the same route.

When you call this operation, take note of the following limits:

- The combinations of ExternalIp, ExternalPort, and Protocol used in DNAT entries must be unique. Requests cannot be distributed to more than one Elastic Compute Service (ECS) instance if these requests are originated from the same source IP address, received on the same port, and use the same protocol.
- The combinations of Protocol, InternalIp, and InternalPort used in DNAT entries must be unique.
- If one or more DNAT entries in the DNAT table are in the Pending or Modifying state, you cannot add DNAT entries to the DNAT table.
- The public IP address (ExternalIp) in the DNAT entry, which is used to access the Internet, must meet the following requirements:
  - If you have purchased a NAT service plan before November 3, 2017, the ExternalIp must be a public IP address in the NAT service plan.
  - If you have not purchased a NAT service plan before November 3, 2017, the ExternalIp must be an elastic IP address (EIP) associated with the NAT service plan.
  - You cannot specify the same EIP in both a DNAT entry and an SNAT entry.
- The private IP address (InternalIp) in the DNAT entry must meet the following requirements:
  - The private IP address must belong to the CIDR block of the virtual private cloud (VPC) where the NAT gateway is deployed.
  - The DNAT entry takes effect only when the private IP address is allocated to an ECS instance and the ECS instance is not assigned an EIP. If the private IP address is allocated to a resource other than an ECS instance, such as a high-availability virtual IP addresses (HAVIPs), Server Load Balancer (SLB) instance, or RDS instance, the DNAT entry does not take effect. Consequently, inbound traffic cannot be forwarded to the private IP address.
  - You cannot specify the same EIP in both a DNAT entry and an SNAT entry.
- You can add up to 100 DNAT entries to a DNAT table.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateForwardEntry	The operation that you want to perform. Set the value to **CreateForwardEntry**.
ExternalIp	String	Yes	116.XX.XX.28	The public IP address of the NAT gateway.
ExternalPort	String	Yes	8080	The public port. Valid values: **1 to 65535**.
ForwardTableId	String	Yes	ftb-bp1mbjubq34hlcqpa****	The ID of the DNAT table.
InternalIp	String	Yes	192.XX.XX.1	The destination private IP address.
InternalPort	String	Yes	80	The destination private port. Valid values: **1 to 65535**.
IpProtocol	String	Yes	TCP	The protocol that is used by the ports. Valid values: • **TCP**: forwards TCP packets. • **UDP**: forwards UDP packets. • **Any**: forwards packets of all protocols.
RegionId	String	Yes	cn-qingdao-env17-d0	The ID of the region where the NAT gateway is created. You can call the `DescribeRegions` operation to query the most recent region list.
ForwardEntryName	String	No	ForwardEntry-1	The name of the DNAT entry. The name must be 2 to 128 characters in length, and start with a letter. It cannot start with `http://` or `https://`.
ClientToken	String	No	0c593ea1-3bea-11e9-b96b-88e9fe637****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The ClientToken value can contain only **ASCII** characters and cannot exceed 64 characters in length.
PortBreak	Boolean	No	false	Specifies whether to remove limits on the port range. Valid values: **true**: removes limits on the port range. **false** (default): sets limits on the port range. **Note** When an SNAT entry and a DNAT entry use the same public IP address, and you want to specify a port number greater than 1024, set **PortBreak** to **true**.

Response parameters

Parameter	Type	Example	Description
ForwardEntryId	String	fwd-119smw5tkasdf****	The ID of the DNAT entry.
RequestId	String	A4AEE536-A97A-40EB-9EBE-53A6948A6928	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateForwardEntry
&ExternalIp=116.XX.XX.28
&ExternalPort=8080
&ForwardTableId=ftb-bp1mbjubq34hlcqpa****
&InternalIp=192.XX.XX.1
&InternalPort=80
&IpProtocol=TCP
&RegionId=cn-qingdao-env17-d0
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CreateForwardEntryResponse>
  <RequestId>A4AEE536-A97A-40EB-9EBE-53A6948A6928</RequestId>
  <ForwardEntryId>fwd-119smw5tkasdf****</ForwardEntryId>
</CreateForwardEntryResponse>
```

`JSON` format

```
{
    "CreateForwardEntryResponse": {
        "RequestId": "A4AEE536-A97A-40EB-9EBE-53A6948A6928",
        "ForwardEntryId": "fwd-119smw5tkasdf****"
    }
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
400	InvalidExternalIp.Malformed	The specified ExternalIp is not a valid IP address.	The error message returned because the specified IP address is invalid.
400	InvalidInternalIp.Malformed	The specified InternalIp is not a valid IP address.	The error message returned because the specified private IP address is invalid.
400	InvalidExternalPort.Malformed	The specified ExternalPort is not a valid port.	The error message returned because the specified public port is invalid.
400	InvalidInternalPort.Malformed	The specified InternalPort is not a valid port.	The error message returned because the specified private port is invalid.
400	Forbidden.DestnationIpOutOfVpcCIDR	The specified Internal Ip is Out of VPC CIDR.	The error message returned because the specified private IP address does not fall within the CIDR block of the VPC. Enter a private IP address that falls within the CIDR block of the VPC.
400	InvalidProtocal.ValueNotSupported	The specified IpProtocol does not support.	The error message returned because the specified protocol is not supported.
400	IncorretForwardEntryStatus	Some Forward entry status blocked this operation..	The error message returned because you are not authorized to perform the specified operation. The error message returned because one or more DNAT entries in the DNAT table are in the Pending or Modifying state.
404	InvalidForwardTableId.NotFound	Specified forward table does not exist.	The error message returned because the specified DNAT table does not exist. Check the parameter value and try again.
404	InvalidExternalIp.NotFound	Specified External Ip address does not found on the VRouter	The error message returned because the specified public IP address does not exist.
400	Forbidden.ExternalIp.UsedInSnatTable	The specified ExternalIp is already used in SnatTable	The error message returned because the specified public IP address is already used by an SNAT entry. Select a different IP address or delete the SNAT entry.
400	Forbindden	The specified Instance already bind eip	The error message returned because the ECS instance is associated with an EIP. Disassociate the EIP from the ECS instance before you create forwarding rules.
400	Forbidden.InternalIpOutOfVpcCIDR	The specified Internal Ip is Out of VPC CIDR.	The error message returned because the private IP address does not fall within the CIDR block of the VPC.
400	Invalid.natgwNotExist	The specified natgateway not exist.	The error message returned because the specified NAT gateway does not exist.
400	InvalidIp.NotInNatgw	The specified Ip not belong to natgateway.	The error message returned because the specified IP address is not associated with the NAT gateway.
400	MissingParameter	Missing mandatory parameter	The error message returned because one or more required parameters are not set. Check whether you have set all required parameters.
500	InternalError	The request processing has failed due to some unknown error.	The error message returned because an unknown error occurred.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name is invalid.

6.6.2. DeleteForwardEntry

Deletes a DNAT entry.

> **Note** You cannot delete DNAT entries if one or more DNAT entries in the DNAT table are in the **Pending** or **Modifying** state.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteForwardEntry	The operation that you want to perform. Set the value to **DeleteForwardEntry**.
ForwardEntryId	String	Yes	fwd-8vbn3bc8roygjp0g****	The ID of the DNAT entry.
ForwardTableId	String	Yes	ftb-8vbx8xu2lqj9qb334****	The ID of the DNAT table.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed. You can call the `DescribeRegions` operation to query the most recent region list.
ClientToken	String	No	123e4567-e89b-12d3-a456-42665544****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Example	Description
RequestId	String	0ED8D006-F706-4D23-88ED-E11ED28DCAC0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteForwardEntry
&ForwardEntryId=fwd-8vbn3bc8roygjp0g****
&ForwardTableId=ftb-8vbx8xu2lqj9qb334****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DeleteForwardEntryResponse>
  <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeleteForwardEntryResponse>
```

`JSON` format

```
{"RequestId":"0ED8D006-F706-4D23-88ED-E11ED28DCAC0"}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
400	IncorretForwardEntryStatus	Some Forward entry status blocked this operation..	The error message returned because you are not authorized to perform the specified operation. The error message returned because one or more DNAT entries in the DNAT table are in the Pending or Modifying state.
404	InvalidForwardEntryId.NotFound	Specified forward entry ID does not exist	The error message returned because the specified DNAT entry does not exist.
404	InvalidForwardTableId.NotFound	Specified forward table does not exist.	The error message returned because the specified DNAT table does not exist. Check the parameter value and try again.
400	IncorretForwardEntryStatus	The Specified forwardEntry is not exist	The error message returned because the specified DNAT entry does not exist.
400	MissingParameter	Missing mandatory parameter	The error message returned because one or more required parameters are not set. Check whether you have set all required parameters.

6.6.3. ModifyForwardEntry

Modifies a specified DNAT entry.

Usage notes

You cannot modify a DNAT entry if it is in the **Pending** or **Modifying** state.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyForwardEntry	The operation that you want to perform. Set the value to **ModifyForwardEntry**.
ForwardEntryId	String	Yes	fwd-8vbn3bc8roygjp0gy****	The ID of the DNAT entry.
ForwardTableId	String	Yes	ftb-8vbx8xu2lqj9qb334****	The ID of the DNAT table.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the NAT gateway. You can call the `DescribeRegions` operation to query the most recent region list.
ExternalIp	String	No	116.28.XX.XX	The public IP address.
ExternalPort	String	No	80	The public port. Valid values: **1** to **65535**.
InternalIp	String	No	192.168.XX.XX	The destination private IP address.
InternalPort	String	No	80	The destination private port. Valid values: **1** to **65535**.
IpProtocol	String	No	TCP	The protocol type. Valid values: • **TCP**: forwards TCP packets. • **UDP**: forwards UDP packets. • **Any**: forwards packets of all protocols.
ForwardEntryName	String	No	ForwardEntry-1	The name of the DNAT entry. The name must be 2 to 128 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	123e4567-e89b-12d3-a456-426655440000	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that the value is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length. **Note** If you do not set this parameter, the system automatically uses **RequestId** as **ClientToken**. **RequestId** of each API request may be different.

Response parameters

Parameter	Type	Example	Description
RequestId	String	24CC85DC-7700-4F09-9624-99E988C7DD03	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyForwardEntry
&ForwardEntryId=fwd-8vbn3bc8roygjp0gy****
&ForwardTableId=ftb-8vbx8xu2lqj9qb334****
&RegionId= cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyForwardEntryResponse>
  <RequestId>24CC85DC-7700-4F09-9624-99E988C7DD03</RequestId>
</ModifyForwardEntryResponse>
```

`JSON` format

```
{
    "RequestId": "24CC85DC-7700-4F09-9624-99E988C7DD03"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
400	InvalidExternalIp.Malformed	The specified ExternalIp is not a valid IP address.	The error message returned because the specified elastic IP address (EIP) is invalid.
400	InvalidInternalIp.Malformed	The specified InternalIp is not a valid IP address.	The error message returned because the specified destination private IP address is invalid.
400	InvalidExternalPort.Malformed	The specified ExternalPort is not a valid port.	The error message returned because the specified public port is invalid.
400	InvalidInternalPort.Malformed	The specified InternalPort is not a valid port.	The error message returned because the specified private port is invalid.
400	Forbidden.DestnationIpOutOfVpcCIDR	The specified Destination Ip is Out of VPC CIDR.	The error message returned because the specified private IP address does not fall within the CIDR block of the virtual private cloud (VPC). Enter a private IP address that falls within the CIDR block of the VPC.
400	InvalidProtocal.ValueNotSupported	The specified IpProtocol does not support.	The error message returned because the specified protocol is not supported.
400	IncorretForwardEntryStatus	Some Forward entry status blocked this operation..	The error message returned because you are not authorized to perform the specified operation. The error message returned because one or more DNAT entries in the DNAT table are in the Pending or Modifying state.
400	QuotaExceeded	Forward entry quota exceeded in this route table.	The error message returned because the number of custom route entries in the same route table cannot exceed 200. Go to the Quota Management page to request a quota increase.
404	InvalidForwardEntryId.NotFound	Specified forward entry ID does not exist	The error message returned because the specified DNAT entry does not exist.
404	InvalidExternalIp.NotFound	Specified External Ip address does not found on the VRouter	The error message returned because the specified EIP does not exist.
404	InvalidForwardTableId.NotFound	Specified forward table does not exist.	The error message returned because the specified DNAT table does not exist. Check the parameter and try again.
400	Forbidden.ExternalIp.UsedInSnatTable	The specified ExternalIp is already used in SnatTable	The error message returned because the specified EIP is already used by an SNAT entry. Select a different EIP or delete the SNAT entry.
400	Forbidden.Already.Bounded	The specified instance already bounded	The error message returned because the specified instance is associated with another DNAT entry.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name format is invalid. Enter the name in the valid format.

6.6.4. DescribeForwardTableEntries

Queries DNAT entries.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeForwardTableEntries	The operation that you want to perform. Set the value to **DescribeForwardTableEntries**.
ForwardTableId	String	Yes	ftb-bp1mbjubq34hlcqpa****	The ID of the DNAT table.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is created. You can call the `DescribeRegions` operation to query the most recent region list.
ForwardEntryId	String	No	fwd-8vbn3bc8roygjp0gy****	The ID of the DNAT entry that is automatically assigned.
ExternalIp	String	No	116.XX.XX.28	The public IP address of the NAT gateway.
ExternalPort	String	No	8080	The public port. Valid values: **1** to **65535**.
InternalIp	String	No	192.XX.XX.1	The destination private IP address.
InternalPort	String	No	80	The destination private port. Valid values: **1** to **65535**.
IpProtocol	String	No	TCP	The protocol type. Valid values: • **TCP**: forwards TCP packets. • **UDP**: forwards UDP packets. • **Any**: forwards packets of all protocols.
ForwardEntryName	String	No	ForwardEntry-1	The name of the DNAT entry. The name must be 2 to 128 characters in length. It must start with a letter and cannot start with `http://` or `https://`.
PageNumber	Integer	No	1	The number of the page to return. Default value: **1**.
PageSize	Integer	No	10	The number of entries to return on each page. Maximum value: **50**. Default value: **10**.

Response parameters

Parameter	Type	Example	Description
ForwardTableEntries	Array of ForwardTableEntry		The details of the DNAT entries.
ForwardTableEntry			
ExternalIp	String	116.XXX.XX.28	The public IP address of the NAT gateway.
ExternalPort	String	80	The public port.
ForwardEntryId	String	fwd-119smw5tk****	The ID of the DNAT entry.
ForwardEntryName	String	ForwardEntry-1	The name of the DNAT entry.
ForwardTableId	String	ftb-11tc6xgmv****	The ID of the DNAT table to which the DNAT entry belongs.
InternalIp	String	192.XX.XX.1	The private IP address.
InternalPort	String	25	The destination private port. Valid values: **1** to **65535**.
IpProtocol	String	TCP	The protocol type.
Status	String	Available	The state of the DNAT entry.
TotalCount	Integer	5	The total number of entries returned.
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	A6C4A8B1-7561-4509-949C-20DEB40D71E6	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeForwardTableEntries
&ForwardTableId=ftb-bp1mbjubq34hlcqpa****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeForwardTableEntriesResponse>
  <TotalCount>5</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>A6C4A8B1-7561-4509-949C-20DEB40D71E6</RequestId>
  <PageNumber>1</PageNumber>
  <ForwardTableEntries>
        <Status>Available</Status>
        <ExternalPort>80</ExternalPort>
        <ExternalIp>116.XXX.XX.28</ExternalIp>
        <ForwardEntryId>fwd-119smw5tk****</ForwardEntryId>
        <IpProtocol>TCP</IpProtocol>
        <InternalPort>25</InternalPort>
        <ForwardEntryName>ForwardEntry-1</ForwardEntryName>
        <InternalIp>192.XX.XX.1</InternalIp>
        <ForwardTableId>ftb-11tc6xgmv****</ForwardTableId>
  </ForwardTableEntries>
</DescribeForwardTableEntriesResponse>
```

`JSON` format

```
{
    "TotalCount": 5,
    "PageSize": 10,
    "RequestId": "A6C4A8B1-7561-4509-949C-20DEB40D71E6",
    "PageNumber": 1,
    "ForwardTableEntries": {
        "Status": "Available",
        "ExternalPort": 80,
        "ExternalIp": "116.XXX.XX.28",
        "ForwardEntryId": "fwd-119smw5tk****",
        "IpProtocol": "TCP",
        "InternalPort": 25,
        "ForwardEntryName": "ForwardEntry-1",
        "InternalIp": "192.XX.XX.1",
        "ForwardTableId": "ftb-11tc6xgmv****"
    }
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
400	IncorretForwardEntryStatus	Some Forward entry status blocked this operation..	The error message returned because you are not authorized to perform the specified operation. One or more DNAT entries in the DNAT table are in the Pending or Modifying state.
404	InvalidForwardTableId.NotFound	Specified forwardTableId does not exist	The error message returned because the specified DNAT table does not exist. Check the parameter value and try again.

6.7. SNAT tables

6.7.1. CreateSnatEntry

Adds an SNAT entry to an SNAT table.

Description

When you call this operation, take note of the following limits:

- The vSwitch and the Elastic Compute Service (ECS) instance specified in the SNAT entry must belong to the virtual private cloud (VPC) where the NAT gateway is deployed.
- Each vSwitch or ECS instance can be specified in only one SNAT entry.
- If a high-availability virtual IP address (HAVIP) exists in the vSwitch, you cannot create SNAT entries.
- You cannot specify the same EIP in both a DNAT entry and an SNAT entry.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateSnatEntry	The operation that you want to perform. Set the value to **CreateSnatEntry**.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed. You can call the `DescribeRegions` operation to query the most recent region list.
SnatIp	String	Yes	47.XX.XX.98	The public IP addresses. Separate multiple IP addresses with commas (,).
SnatTableId	String	Yes	stb-bp190wu8io1vgev****	The ID of the SNAT table.
SourceVSwitchId	String	No	vsw-bp1nhx2s9ui5o****	The ID of the vSwitch that requires to access the Internet.
SourceCIDR	String	No	10.1.1.0/24	The CIDR block of the vSwitch or the IP address of the ECS instance. • vSwitch granularity: specifies the CIDR block of the vSwitch, for example, 192.168.1.0/24. When an ECS instance of a vSwitch requires to access the Internet, the NAT gateway provides the SNAT service for the ECS instance. If you specify only one public IP address in the **SnatIp** parameter, the ECS instance uses the specified public IP address to access the Internet. If you specify multiple public IP addresses in the **SnatIp** parameter, the ECS instance randomly selects a public IP address from **SnatIp** to access the Internet. • ECS granularity: specifies the IP address of the ECS instance, for example, 192.168.1.0/32. When the ECS instance requires to access the Internet, the NAT gateway provides the SNAT service for the ECS instance. If you specify only one public IP address in the **SnatIp** parameter, the ECS instance uses the specified public IP address to access the Internet. If you specify multiple public IP addresses in the **SnatIp** parameter, the ECS instance randomly selects a public IP address from **SnatIp** to access the Internet. This parameter and the **SourceVSwtichId** parameter cannot be set at the same time. If the **SourceVSwitchId** parameter is set, you cannot set the **SourceCIDR** parameter. If the **SourceCIDR** parameter is set, you cannot set the **SourceVSwitchId** parameter.
SnatEntryName	String	No	SnatEntry-1	The name of the SNAT entry. The name must be 2 to 128 characters in length, and must start with a letter. It cannot start with `http://` or `https://`.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-001****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. `ClientToken` can contain only ASCII characters and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Example	Description
SnatEntryId	String	snat-kmd6nv8fy****	The ID of the SNAT entry.
RequestId	String	2315DEB7-5E92-423A-91F7-4C1EC9AD97C3	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateSnatEntry
&RegionId=cn-qingdao-env17-d01
&SnatIp=47.XX.XX.98
&SnatTableId=stb-bp190wu8io1vgev****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CreateSnatEntryResponse>
      <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
      <SnatEntryId>snat-119smw5tkx****</SnatEntryId>
</CreateSnatEntryResponse>
```

`JSON` format

```
{
    "SnatEntryId": "snat-kmd6nv8fyx****",
    "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidSnatTableId.NotFound	Specified SNAT table does not exist.	The error message returned because the specified SNAT table does not exist. Check whether the ID of the SNAT table is valid.
400	Forbidden.SourceVSwitchId.Include HaVip	There is some HaVips under specified VSwitch	The error message returned because the specified vSwitch is associated with HAVIPs.
400	InvalidSnatIp.Malformed	The specified SnatIp is not a valid IP address.	The error message returned because the specified public IP address is invalid.
400	SNAT_IP_POOL_COUNT_TOO_MANY	The Snat pool ip too many.	The error message returned because the number of IP addresses in the SNAT IP address pool has reached the upper limit.
400	Forbidden.SnatEntryCountLimited	SNAT entry in the specified SNAT table reach it?s limit.	The error message returned because the number of SNAT entries has reached the upper limit.
400	NOT_ALLOW_USE_SOURCECIDR	The User not in nat_scope_unlimited white list. Cannot use SourceCidr param.	The error message returned because the specified private IP address does not fall within the CIDR block of the VPC.
404	InvalidVSwitchId.NotFound	The specified virtual switch does not exists.	The error message returned because the specified vSwitch does not exist. Check whether the specified ID is valid.
400	INVALID_PARAMETER	The parameter invalid.	The error message returned because the specified parameter is invalid.
400	Forbidden.SourceVSwitchId.Duplicated	The specified SourceCIDRis duplicated.	The error message returned because an SNAT entry is already created for the specified vSwitch.
404	InvalidSnatIp.NotFound	Specified SnatIp does not found on the NAT Gateway	The error message returned because the specified public IP address is not found on the NAT gateway.
400	Forbidden.IpUsedInForwardTable	The specified SnatIp already used in forward table	The error message returned because the specified public IP address is already used by a DNAT entry. Select another public IP address or delete the DNAT entry.
400	Forbindden	The specified Instance already bind eip	The error message returned because the ECS instance is associated with an EIP. Disassociate the EIP from the ECS instance before you create forwarding rules.
400	OperationUnsupported.CidrConflict	The specified CIDR block conflicts with an existing SNAT entry.	The error message returned because the specified CIDR block conflicts with those in existing SNAT entries.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name is invalid.

6.7.2. DeleteSnatEntry

Deletes a specified SNAT entry.

> **Note** You cannot delete SNAT entries if one or more SNAT entries in the SNAT table are in the **Pending** or **Modifying** state.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteSnatEntry	The operation that you want to perform. Set the value to **DeleteSnatEntry**.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed. You can call the `DescribeRegions` operation to query the most recent region list.
SnatEntryId	String	Yes	snat-bp1vcgcf8tm0plqc****	The ID of the SNAT entry.
SnatTableId	String	Yes	stb-bp190wu8io1vgev80****	The ID of the SNAT table.
ClientToken	String	No	123e4567-e89b-12d3-a456-42665544****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can only contain ASCII characters and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Example	Description
RequestId	String	47B80B6A-759A-479C-A565-76D04BDA29F3	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteSnatEntry
&RegionId=cn-qingdao-env17-d01
&SnatEntryId=snat-bp1vcgcf8tm0plqc****
&SnatTableId=stb-bp190wu8io1vgev80****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DeleteSnatEntryResponse>
  <RequestId>47B80B6A-759A-479C-A565-76D04BDA29F3</RequestId>
</DeleteSnatEntryResponse>
```

`JSON` format

```
{"RequestId":"47B80B6A-759A-479C-A565-76D04BDA29F3"}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
400	IncorretSnatEntryStatus	Some Snat entry status blocked this operation..	The error message returned because you are not authorized to perform the specified operation. The error message returned because one or more SNAT entries in the SNAT table are in the Pending or Modifying state.
404	InvalidSnatEntryId.NotFound	Specified Snat entry ID does not exist	The error message returned because the specified SNAT entry does not exist. Check whether the SNAT entry is valid.
404	InvalidSnatTableId.NotFound	Specified SNAT table does not exist.	The error message returned because the specified SNAT table does not exist. Check whether the ID of the SNAT table is valid.
404	InvalidSnatEntryId.NotFound	Specified SNAT entry does not exist.	The error message returned because the specified SNAT entry does not exist. Check whether the SNAT entry is valid.

6.7.3. ModifySnatEntry

Modifies a specified SNAT entry.

> **Note** You cannot modify SNAT entries if one or more SNAT entries in the SNAT table are in the **Pending** or **Modifying** state.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifySnatEntry	The operation that you want to perform. Set the value to **ModifySnatEntry**.
RegionId	String	Yes	cn-qingdao-env17-d0	The ID of the region where the NAT gateway is deployed.
SnatEntryId	String	Yes	snat-bp1vcgcf8tm0plqcg****	The ID of the SNAT entry.
SnatTableId	String	Yes	stb-8vbczigrhop8x5u3t****	The ID of the SNAT table to which the SNAT entry belongs.
SnatIp	String	Yes	47.XX.XX.98	The public IP address in the SNAT entry. If multiple IP addresses are specified, separate them with commas (,).
SnatEntryName	String	No	SnatEntry-1	The name of the SNAT entry. The description must be 2 to 128 characters in length, and start with a letter. It cannot start with `http://` or `https://`.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-001****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. Only ASCII characters are allowed. It can contain up to 64 ASCII characters.

Response parameters

Parameter	Type	Example	Description
RequestId	String	2315DEB7-5E92-423A-91F7-4C1EC9AD97C3	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifySnatEntry
&RegionId=cn-qingdao-env17-d0
&SnatEntryId=snat-bp1vcgcf8tm0plqcg****
&SnatTableId=stb-8vbczigrhop8x5u3t****
&SnatIp=47.XX.XX.98
&<Common request parameters>
```

Successful response examples

`XML` format

```
<ModifySnatEntryResponse>
      <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</ModifySnatEntryResponse>
```

`JSON` format

```
{
  "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID is invalid. Check whether the service is available in the specified region.
404	InvalidSnatTableId.NotFound	Specified SNAT table does not exist.	The error message returned because the specified SNAT table does not exist. Check whether the ID of the SNAT table is valid.
400	InvalidSnatIp.Malformed	The specified SnatIp is not a valid IP address.	The error message returned because the specified public IP address is invalid.
404	InvalidSnatEntryId.NotFound	Specified SNAT entry does not exist.	The error message returned because the specified SNAT entry does not exist. Check whether the SNAT entry is valid.
400	Forbidden.SourceVSwitchId.Duplicated	The specified SourceCIDRis duplicated.	The error message returned because an SNAT entry is already configured for the specified vSwitch.

HttpCode	Error code	Error message	Description
404	InvalidSnatIp.NotFound	Specified SnatIp does not found on the NAT Gateway	The error message returned because the specified public IP address does not exist in the NAT gateway.
400	Forbidden.IpUsedInForwardTable	The specified SnatIp already used in forward table	The error message returned because the specified public IP address is already used by a DNAT entry. Select another IP address or delete the DNAT rule that uses the public IP address.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name format is invalid.

6.7.4. DescribeSnatTableEntries

Queries SNAT entries.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSnatTableEntries	The operation that you want to perform. Set the value to **DescribeSnatTableEntries**.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where the NAT gateway is deployed. You can call the `DescribeRegions` operation to query the most recent region list.
SnatTableId	String	Yes	stb-8vbczigrhop8x5u3t****	The ID of the SNAT table.
SnatEntryId	String	No	snat-8vbae8uqh7rjpk7d2****	The ID of the SNAT entry.
SourceVSwitchId	String	No	vsw-3xb****	The ID of the vSwitch that can access the Internet through SNAT.
SourceCIDR	String	No	116.XX.XX.0/28	The source CIDR block of the SNAT entry.
SnatIp	String	No	116.XX.XX.28	The public IP address in the SNAT entry.
SnatEntryName	String	No	SnatEntry-1	The name of the SNAT entry. The name must be 2 to 128 characters in length, and start with a letter. The name cannot start with `http://` or `https://`.
PageNumber	Integer	No	1	The number of the page to return. Default value: **1**.
PageSize	Integer	No	10	The number of entries to return on each page. Maximum value: **50**. Default value: **10**.

Response parameters

Parameter	Type	Example	Description
SnatTableEntries	Array of SnatTableEntry		The detailed information about the SNAT entries.
SnatTableEntry			
SnatEntryId	String	snat-8vbae8uqh7rjpk7d2****	The ID of the SNAT entry.
SnatEntryName	String	SnatEntry-1	The name of the SNAT entry.
SnatIp	String	116.XX.XX.28	The public IP address in the SNAT entry.
SnatTableId	String	stb-8vbczigrhop8x5u3t****	The ID of the SNAT table to which the SNAT entry belongs.
SourceCIDR	String	116.XX.XX.0/28	The source CIDR block of the SNAT entry.
SourceVSwitchId	String	vsw-3xb****	The ID of the vSwitch that can access the Internet through SNAT.

Parameter	Type	Example	Description
Status	String	Pending	The state of the SNAT entry.
TotalCount	Integer	1	The number of entries returned.
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	5	The number of entries returned on each page.
RequestId	String	6D7E89B1-1C5B-412B-8585-4908E222EED5	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSnatTableEntries
&RegionId=cn-qingdao-env17-d01
&SnatTableId=stb-8vbczigrhop8x5u3t****
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeSnatTableEntriesResponse>
  <TotalCount>1</TotalCount>
  <PageSize>5</PageSize>
  <RequestId>6D7E89B1-1C5B-412B-8585-4908E222EED5</RequestId>
  <PageNumber>1</PageNumber>
  <SnatTableEntries>
        <Status>Pending</Status>
        <SourceVSwitchId>vsw-3xb****</SourceVSwitchId>
        <SnatEntryName>SnatEntry-1</SnatEntryName>
        <SourceCIDR>116.XX.XX.0/28</SourceCIDR>
        <SnatEntryId>snat-8vbae8uqh7rjpk7d2****</SnatEntryId>
        <SnatIp>116.XX.XX.28</SnatIp>
        <SnatTableId>stb-8vbczigrhop8x5u3t****</SnatTableId>
  </SnatTableEntries>
</DescribeSnatTableEntriesResponse>
```

`JSON` format

```
{
    "TotalCount": 1,
    "PageSize": 5,
    "RequestId": "6D7E89B1-1C5B-412B-8585-4908E222EED5",
    "PageNumber": 1,
    "SnatTableEntries": {
        "Status": "Pending",
        "SourceVSwitchId": "vsw-3xb****",
        "SnatEntryName": "SnatEntry-1",
        "SourceCIDR": "116.XX.XX.0/28",
        "SnatEntryId": "snat-8vbae8uqh7rjpk7d2****",
        "SnatIp": "116.XX.XX.28",
        "SnatTableId": "stb-8vbczigrhop8x5u3t****"
    }
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidSnatTableId.NotFound	Specified SNAT table does not exist.	The error message returned because the specified SNAT table does not exist. Check whether the ID of the SNAT table is valid.

6.8. NAT bandwidth packages

6.8.1. CreateBandwidthPackage

Creates a NAT service plan.

Usage notes

A NAT service plan consists of bandwidth resources and public IP addresses. You can associate up to four NAT service plans with a NAT gateway.

A NAT service plan includes:

- Bandwidth resources
- A group of public IP addresses

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateBandwidthPackage	The operation that you want to perform. Set the value to **CreateBandwidthPackage**.
Bandwidth	Integer	Yes	5	The bandwidth of the NAT service plan. Valid values: **5** to **1000**. Unit: Mbit/s.
IpCount	Integer	Yes	2	The number of public IP addresses in the NAT service plan. Valid values: **1 to 50**.
NatGatewayId	String	Yes	ngw-7mwb327j1****	The ID of the NAT gateway.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the NAT service plan. You can call the `DescribeRegions` operation to query the most recent region list.
Name	String	No	Name	The name of the NAT service plan. The name must be 2 to 128 characters in length and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter. It cannot start with `http://` or `https://`.
Description	String	No	Description	The description of the NAT service plan. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-001****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that the value is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length. **Note** If you do not set this parameter, the system automatically uses **RequestId** as **ClientToken**. **RequestId** of each API request may be different.
ISP	String	No	BGP	Only **BGP** is supported.
Zone	String	No	cn-qingdao-env17-amtest11001-a	The zone to which the NAT service plan belongs. If you do not set this parameter, the service plan is randomly allocated to a zone. **Note** Connectivity is not affected when the IP addresses provided by the NAT service plan and the backend Elastic Compute Service (ECS) instances belong to different zones. However, when the IP addresses and ECS instances belong to the same zone, latency can be reduced.
InternetChargeType	String	No	PayByBandwidth	The metering method of the NAT service plan. Valid values: - **PayByTraffic**: pay-by-data-transfer - **PayByBandwidth**: pay-by-bandwidth

Response parameters

Parameter	Type	Example	Description
BandwidthPackageId	String	bwp-s6lmotmkk****	The ID of the NAT service plan.
RequestId	String	54ED4074-3F89-4F11-B166-837DD3E20FE3	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateBandwidthPackage
&Bandwidth=5
&IpCount=2
&NatGatewayId=ngw-7mwb327j1****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CreateBandwidthPackageResponse>
  <RequestId>54ED4074-3F89-4F11-B166-837DD3E20FE3</RequestId>
  <BandwidthPackageId>bwp-s61motmkk****</BandwidthPackageId>
</CreateBandwidthPackageResponse>
```

`JSON` format

```
{
    "RequestId": "54ED4074-3F89-4F11-B166-837DD3E20FE3",
    "BandwidthPackageId": "bwp-s61motmkk****"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidVpcId.NotFound	Specified value of VpcId is not found in our record.	The error message returned because the specified virtual private cloud (VPC) does not exist. Check whether the specified VPC is valid.
400	MissingParameter	Miss mandatory parameter.	The error message returned because some required parameters are not set. Check whether you have set all required parameters before you call this operation.
404	InvalidZoneId.NotFound	Specified value of ZoneId is not exists.	The error message returned because the specified zone does not exist.
404	InvalidZoneId.NotFound	Can not find ZoneId for allocated ip.	The error message returned because the zone of the specified IP address is invalid.
400	QuotaExceeded.BandwidthPackageIps	The specified ipCount exceeded quota.	The error message returned because the number of IP addresses has reached the upper limit. Request a quota increase on the Quota Management page.
400	QuotaExceeded.BandwidthPackageCountOnNatGateway	BandwidthPackage count limit on one NatGateway exceeded.	The error message returned because the number of NAT service plans has reached the upper limit. You can associate up to four NAT service plans with a NAT gateway.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name format is invalid. Enter the name in the valid format.
400	InvalidParameter.Description.Malformed	The specified Description is not valid.	The error message returned because the specified description is invalid.
400	InvalidParameter.BandwidthPackage.n.ISP.ValueNotSupport	The specified ISP of BandwidthPackage is not valid.	The error message returned because the specified Internet service provider (ISP) of the EIP bandwidth plan is invalid.
400	ZONE_NO_AVAILABLE_IP	The Zone have no available ip.	The error message returned because no IP address is available in the zone.

6.8.2. ModifyBandwidthPackageSpec

Modifies the bandwidth value of a specified NAT service plan.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyBandwidthPackageSpec	The operation that you want to perform. Set the value to **ModifyBandwidthPackageSpec**.

Parameter	Type	Required	Example	Description
Bandwidth	String	Yes	5	The bandwidth of the NAT service plan. Valid values: **5** to **1000**. Unit: Mbit/s.
BandwidthPackageId	String	Yes	bwp-s6lmotmkk****	The ID of the NAT service plan.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the NAT service plan. You can call the `DescribeRegions` operation to query the most recent region list.

Response parameters

Parameter	Type	Example	Description
RequestId	String	079874CD-AEC1-43E6-AC03-ADD96B6E4907	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyBandwidthPackageSpec
&Bandwidth=5
&BandwidthPackageId=bwp-s6lmotmkk****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyBandwidthPackageSpecResponse>
  <RequestId>079874CD-AEC1-43E6-AC03-ADD96B6E4907</RequestId>
</ModifyBandwidthPackageSpecResponse>
```

`JSON` format

```
{
    "RequestId": "079874CD-AEC1-43E6-AC03-ADD96B6E4907"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidBandwidth.ValueNotSupported	The specified value of Bandwidth not supported.	The error message returned because the specified maximum bandwidth value is invalid.
404	BandwidthPackage.FinancialLocked	The specified BandwidthPackage has been Financail Lock.	The error message returned because the specified NAT service plan is locked due to overdue payments.

6.8.3. DescribeBandwidthPackages

Queries NAT service plans in a specified region.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeBandwidthPackages	The operation that you want to perform. Set the value to **DescribeBandwidthPackages**.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the NAT gateway. You can call the `DescribeRegions` operation to query the most recent region list.
BandwidthPackageId	String	No	bwp-bp1xea10o8qxwdfs****	The ID of the NAT service plan.
NatGatewayId	String	No	ngw-bp1uewa15k4iydfre****	The ID of the NAT gateway.

Parameter	Type	Required	Example	Description
PageNumber	Integer	No	10	The number of the page to return. Default value: **1**.
PageSize	Integer	No	10	The number of entries to return on each page. Maximum value: **50**. Default value: **10**.

Response parameters

Parameter	Type	Example	Description
BandwidthPackages	Array of BandwidthPackage		The details about the NAT service plan.
BandwidthPackage			
Bandwidth	String	5	The maximum bandwidth. Valid values: **5** to **5000**. Unit: Mbit/s.
BandwidthPackageId	String	bwp-xxoo123sfwr****	The ID of the NAT service plan.
BusinessStatus	String	Normal	The status of the bandwidth plan. Valid values: • **Normal**: normal • **FinancialLocked**: locked due to overdue payments • **SecurityLocked**: locked for security reasons
CreationTime	String	2017-06-08T12:20:55	The time when the NAT gateway was created. The time follows the ISO 8601 standard in the YYYY-MM-DDThh:mmZ format. The time is displayed in UTC.
Description	String	test123	The description of the instance. The description must be 2 to 256 characters in length. The description is displayed in the console. This parameter is empty by default. The description cannot start with `http://` or `https://`.
ISP	String	BGP	Only **BGP** is supported.
InstanceChargeType	String	PostPaid	The billing method of the instance. Only **PostPaid** (pay-as-you-go) is supported.
InternetChargeType	String	PayByBandwidth	The metering method. • **PayByTraffic**: pay-by-data-transfer • **PayByBandwidth**: pay-by-bandwidth
IpCount	String	1	The number of public IP addresses in the NAT service plan. Valid values: **1** to **50**.
Name	String	abc	The name of the NAT service plan.
NatGatewayId	String	ngw-xxoo123ggtf****	The ID of the NAT gateway.
PublicIpAddresses	Array of PublicIpAddresse		The IP address in the NAT service plan.
PublicIpAddresse			
AllocationId	String	eip-2zeerraiwb7ujdeds****	The ID that is allocated.
ApAccessEnabled	Boolean	true	Indicates whether access points are used.
IpAddress	String	116.52.XX.XX	The IP address.
UsingStatus	String	Available	The usage status.
RegionId	String	cn-qingdao-env17-d01	The region ID of the NAT service plan.

Parameter	Type	Example	Description
Status	String	Available	The status of the bandwidth plan.
ZoneId	String	cn-qingdao-env17-amtest11001-a	The ID of the zone to which the NAT service plan belongs.
TotalCount	Integer	10	The number of entries returned.
PageNumber	Integer	10	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	4EC47282-1B74-4534-BD0E-403F3EE64CAF	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeBandwidthPackages
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeBandwidthPackagesResponse>
  <TotalCount>10</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>4EC47282-1B74-4534-BD0E-403F3EE64CAF</RequestId>
  <PageNumber>10</PageNumber>
  <BandwidthPackages>
        <Status>Available</Status>
        <IpCount>1</IpCount>
        <Description>test123</Description>
        <ZoneId>cn-qingdao-env17-amtest11001-a</ZoneId>
        <InstanceChargeType>PostPaid</InstanceChargeType>
        <ISP>BGP</ISP>
        <BusinessStatus>Normal</BusinessStatus>
        <InternetChargeType>PayByBandwidth</InternetChargeType>
        <Name>abc</Name>
        <Bandwidth>5</Bandwidth>
        <CreationTime>2017-06-08T12:20:55</CreationTime>
        <BandwidthPackageId>bwp-xxoo123sfwr****</BandwidthPackageId>
        <RegionId>cn-qingdao-env17-d01</RegionId>
        <NatGatewayId> ngw-xxoo123ggtf****</NatGatewayId>
        <PublicIpAddresses>
              <UsingStatus>Available</UsingStatus>
              <ApAccessEnabled>true</ApAccessEnabled>
              <AllocationId>eip-2zeerraiwb7ujdeds****</AllocationId>
              <IpAddress>116.52.XX.XX</IpAddress>
        </PublicIpAddresses>
  </BandwidthPackages>
</DescribeBandwidthPackagesResponse>
```

`JSON` format

```
{
    "TotalCount": 10,
    "PageSize": 10,
    "RequestId": "4EC47282-1B74-4534-BD0E-403F3EE64CAF",
    "PageNumber": 10,
    "BandwidthPackages": {
        "Status": "Available",
        "IpCount": 1,
        "Description": "test123",
        "ZoneId": "cn-qingdao-env17-amtest11001-a",
        "InstanceChargeType": "PostPaid",
        "ISP": "BGP",
        "BusinessStatus": "Normal",
        "InternetChargeType": "PayByBandwidth",
        "Name": "abc",
        "Bandwidth": 5,
        "CreationTime": "2017-06-08T12:20:55",
        "BandwidthPackageId": "bwp-xxoo123sfwr****",
        "RegionId": "cn-qingdao-env17-d01",
        "NatGatewayId": "ngw-xxoo123ggtf****",
        "PublicIpAddresses": {
            "UsingStatus": "Available",
            "ApAccessEnabled": true,
            "AllocationId": "eip-2zeerraiwb7ujdeds****",
            "IpAddress": "116.52.XX.XX"
        }
    }
}
```


Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.

6.8.4. ModifyBandwidthPackageAttribute

Modifies the name and description of a specified NAT service plan.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyBandwidthPackageAttribute	The operation that you want to perform. Set the value to **ModifyBandwidthPackageAttribute**.
BandwidthPackageId	String	Yes	bwp-s6lmotmkk****	The ID of the NAT service plan.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the NAT service plan. You can call the `DescribeRegions` operation to query the most recent region list.
Name	String	No	NATABC	The name of the NAT service plan. The name must be 2 to 128 characters in length and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	This is NAT.	The description of the NAT service plan. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Example	Description
RequestId	String	DFDDD35D-3F29-4E15-AA28-53F5341F9599	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyBandwidthPackageAttribute
&BandwidthPackageId=bwp-s6lmotmkk****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<ModifyBandwidthPackageAttributeResponse>
  <RequestId>DFDDD35D-3F29-4E15-AA28-53F5341F9599</RequestId>
</ModifyBandwidthPackageAttributeResponse>
```

`JSON` format

```
{
    "RequestId": "DFDDD35D-3F29-4E15-AA28-53F5341F9599"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	InvalidBandwidthPackageId.NotFound	The specified bandwidthPackageId does not exist in our records.	The error message returned because the ID of the specified EIP bandwidth plan does not exist.
400	InvalidParameter.Name.Malformed	The specified Name is not valid.	The error message returned because the specified name format is invalid. Enter the name in the valid format.
400	InvalidParameter.Description.Malformed	The specified Description is not valid.	The error message returned because the specified description is invalid.

6.8.5. DeleteBandwidthPackage

Deletes a specified NAT service plan.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteBandwidthPackage	The operation that you want to perform. Set the value to **DeleteBandwidthPackage**.
BandwidthPackageId	String	Yes	bwp-bp1arsrmca9kp****	The ID of the NAT service plan.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the NAT gateway. You can call the `DescribeRegions` operation to query the most recent region list.
Force	Boolean	No	false	Specifies whether to forcefully delete the NAT service plan. Valid values: • **false**(default): no • **true**: yes

Response parameters

Parameter	Type	Example	Description
RequestId	String	7D275A59-1EB0-4775-8A20-2A47055EAC5C	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteBandwidthPackage
&BandwidthPackageId=bwp-bp1arsrmca9kp****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DeleteBandwidthPackageResponse>
  <RequestId>7D275A59-1EB0-4775-8A20-2A47055EAC5C</RequestId>
</DeleteBandwidthPackageResponse>
```

`JSON` format

```
{
    "RequestId": "7D275A59-1EB0-4775-8A20-2A47055EAC5C"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
400	DependencyViolation.ForwardEntry	The specified BandwidthPackageId has dependent resource.	The error message returned because the NAT service plan is associated with SNAT or DNAT entries. Delete them and try again.
400	DependencyViolation.SnatEntry	The specified BandwidthPackageId has dependent resource.	The error message returned because the NAT service plan is associated with SNAT or DNAT entries. Delete them and try again.

6.8.6. RemoveBandwidthPackageIps

Removes public IP addresses from a NAT service plan.

When you call this operation, you must specify the public IP addresses to be removed.

- You cannot remove all public IP addresses. If you specify all public IP addresses, this operation fails.
- If you specify public IP addresses that are not associated with the NAT service plan, this operation fails.
- If you specify public IP addresses that are used in DNAT or SNAT entries, this operation fails.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	RemoveBandwidthPackageIps	The operation that you want to perform. Set the value to **RemoveBandwidthPackageIps**.
BandwidthPackageId	String	Yes	bwp-s6lmotmkk****	The ID of the NAT service plan from which you want to remove the public IP addresses.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the NAT service plan. You can call the `DescribeRegions` operation to query the most recent region list.
RemovedIpAddresses.N	RepeatList	Yes	116.12.XX.XX	The ID of the public IP address to be removed. Valid values of **N**: **1** to **20**.
ClientToken	String	No	123e4567-e89b-12d3-a456-426655440000	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length. **Note** If you do not set this parameter, the system automatically uses **RequestId** as **ClientToken**. **RequestId** may be different for each API request.

Response parameters

Parameter	Type	Example	Description
RequestId	String	7D275A59-1EB0-4775-8A20-2A47055EAC5C	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=RemoveBandwidthPackageIps
&BandwidthPackageId=bwp-s6lmotmkk****
&RegionId=cn-qingdao-env17-d01
&RemovedIpAddresses.1=116.12.XX.XX
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RemoveBandwidthPackageIpsResponse>
  <RequestId>7D275A59-1EB0-4775-8A20-2A47055EAC5C</RequestId>
</RemoveBandwidthPackageIpsResponse>
```

`JSON` format

```
{
    "RequestId": "7D275A59-1EB0-4775-8A20-2A47055EAC5C"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidRegionId.NotFound	The specified RegionId does not exist in our records.	The error message returned because the specified region ID does not exist.
404	invalidRemovedIpAddresses.NotFound	Some of the specified value of RemovedIpAddress not found in specified BandwidthPackage.	The error message returned because a specified public IP address is not associated with the NAT service plan. Check the specified IP addresses.
400	InvalidIpCount.ValueNotSupported	Can not remove all ips of the bandwidthPackage.	The error message returned because you cannot remove all public IP addresses.
400	InvalidRemovedIpAddresses.NotFound	Some of remove ip is not natPublicIp.	The error message returned because one or more specified public IP addresses are not associated with the NAT service plan.
400	DependencyViolation.ForwardEntry	The ip has been used by ForwardEntry.	The error message returned because one or more specified public IP addresses are used by port forwarding rules. Delete the rules before you call this operation.
400	DependencyViolation.SnatEntry	The ip has been used by SnatEntry.	The error message returned because one or more specified public IP addresses are used by SNAT entries. Delete the SNAT entries before you call this operation.
404	BandwidthPackage.FinancialLocked	The specified BandwidthPackage has been Financail Lock.	The error message returned because the specified NAT service plan is locked due to overdue payments.

7.Appendixes

7.1. Use the ASAPI gateway to call API operations

You can use the Apsara Stack API (ASAPI) gateway to call API operations of most Apsara Stack services. This topic describes how to call API operations by using the ASAPI gateway and provides links to references.

Procedure

1. Obtain the ASAPI SDK.

   Before you use ASAPI to call an API operation, you must obtain the ASAPI SDK. For more information, see Obtain the ASAPI SDK.

2. Obtain the endpoint of ASAPI. For more information, see Obtain the endpoint of ASAPI.

3. Obtain an AccessKey pair.

   Obtain the AccessKey pair that is required for calling an API operation.

   > **Note**
   >
   > We recommend that you use the AccessKey pair of a personal account to call the API operations of the Apsara Uni-manager Management Console and cloud services.

4. Obtain the region ID.

   Obtain the region ID that is required for calling an API operation.

5. Obtain the organization ID and resource set ID.

   You can call the GetOrganizationList operation to obtain the organization ID. For more information, see *GetOrganizationList* in *Apsara Uni-manager Management Console Developer Guide*.

   You can call the ListResourceGroup operation to obtain the resource set ID. For more information, see *ListResourceGroup* in *Apsara Uni-manager Management Console Developer Guide*.

   > **Note**
   >
   > When you call an API operation, you can specify the organization ID and resource set ID by using the <x-acs-organizationid> and <x-acs-resourcegroupid> parameters. This allows you to query specified resources.
   >
   > - If you do not set the <x-acs-organizationid> parameter, the organization to which the current user belongs is used by default.
   > - If you do not set the <x-acs-resourcegroupid> parameter, it is empty by default. If you specify a resource set ID, you must also specify an organization ID.

6. Refer to the API reference.

   Obtain the developer guide of the Apsara Stack service that you want to use. You can learn the features of API operations and how to call the API operations. For more information, see Use developer guides.

7. Use ASAPI SDK to call API operations.

   After you complete the preceding steps, you can use the ASAPI SDK to call API operations. For more information about how to use SDKs for different languages, see the relevant topics.

   The following example shows how to call the DescribeInstances operation of Elastic Compute Service (ECS) by using SDK for Java:

```
public static void main(String[] args) {
    ASClient client = new ASClient();
    // Specify the caller. The caller is recorded in logs.
    client.setSdkSource("autoTest");

    // Set request parameters.
    Map<String, Object> parameters = new HashMap<String, Object>();;

    parameters.put("Product", "Ecs");// Specify the POP code, which is the same as the POP code in the corresponding API directory.

    parameters.put("Action", "DescribeInstances"); // Specify the name of the API operation. Use the same letter case as the corresponding API di
rectory.

    parameters.put("Version", "2014-05-26"); // Specify the API version.

    // Specify the region ID that you obtained.
    parameters.put("RegionId", "xxx");

    // Specify your AccessKey ID and AccessKey secret.
    parameters.put("AccessKeyId", "xxx");
    parameters.put("AccessKeySecret", "xxx");

    // Add the parameters based on the API reference. Take note that the parameters are case-sensitive.
    parameters.put("PageNumber",1);
    parameters.put("PageSize",10);

    Map<String,String> headers=new HashMap<>();
    // Specify the organization ID in the Apsara Uni-manager Management Console.
    headers.put("x-acs-organizationid","3");
    // Specify the resource set ID in the Apsara Uni-manager Management Console.
    //headers.put("x-acs-resourcegroupid", "<your-resourcegroupid>");


    // Specify the endpoint of ASAPI.
    String endpoint="https://public.asapi.xxx.xxx/asapi/v3";

    // Initiate the request.
    String result = client.doPost(endpoint,headers, parameters);

    // Display the results.
    System.out.println(JSONObject.toJSONString(JSONObject.parseObject(result), SerializerFeature.PrettyFormat));
}
```

7.2. Use the ASAPI gateway to make API calls

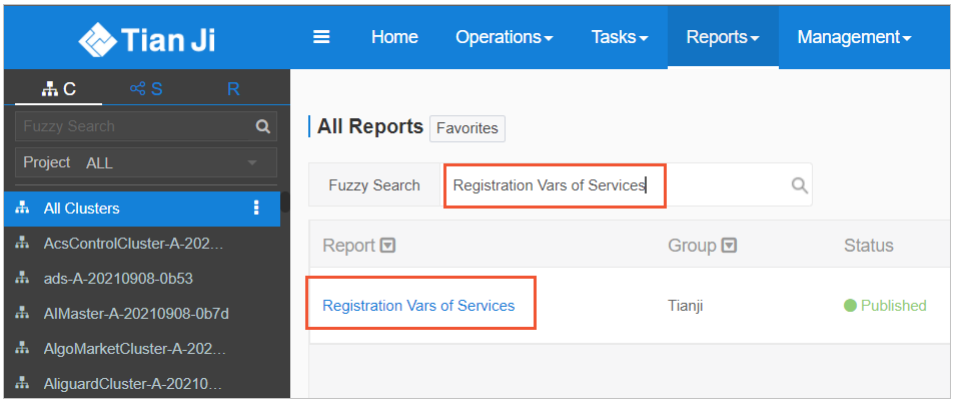
7.2.1. Generate an endpoint for ASAPI

This topic describes three methods that you can use to generate an endpoint for ASAPI. This topic also describes how to verify the endpoint of ASAPI.

Generate an endpoint for ASAPI

Method 1: Use Registration Vars of Services to generate an endpoint

1. Log on to the Apsara Infrastructure Management console.
2. In the left-side navigation pane, click **Reports**.
3. On the **All Reports** page, search for `Registration Vars of Services` and click the report name.



4. On the **Registration Vars of Services** page, click the ☰ icon next to **Service** and enter `asapi` in the search box.

5. Find the asapi service, right-click in the **Service Registration** column, and then select **Show More** from the shortcut menu.

   In the **Details** message, obtain the value of **asapi.public.endpoint**.

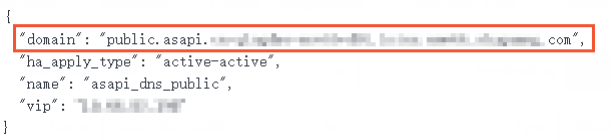
6. Generate an endpoint for ASAPI in the following format:

```
https://<asapi.public.endpoint>/asapi/v3
```

Method 2: Use cluster resources to generate an endpoint

1. Log on to the Apsara Infrastructure Management console.
2. Go to the Cluster Operations page.
   i. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
   ii. In the **Cluster** search box, enter `ascm`.
   iii. Click **Operations** in the **Actions** column.
3. Obtain the value of the domain parameter.
   i. Click the **Cluster Resources** tab.
   ii. In the **Name** field, enter `asapi_dns_public`.
   iii. Click **Details** in the **Application Parameter** column.

   In the **Application Parameter** message, view the value of the **domain** parameter.



4. Generate an endpoint for ASAPI in the following format:

```
https://<domain>/asapi/v3
```

Method 3: Concatenate strings to generate an endpoint

You can also concatenate strings to generate an endpoint in the following format:

```
https://public.asapi.<region>.<internet-domain>/asapi/v3
```

> **Note**
>
> 1. Replace <region> with the actual region ID.
> 2. Replace <internet-domain> with the root domain of your Apsara Stack service. To obtain the root domain, contact Apsara Stack O&M engineers. Take note of this point: Use the internet-domain parameter instead of the intranet-domain parameter.

If the **region** value is `cn-****-****-d01` and the **internet-domain** value is `inter.****.****.com`,

the following sample endpoint is generated:

```
https://public.asapi.cn-****-****-d01.inter.****.****.com/asapi/v3
```

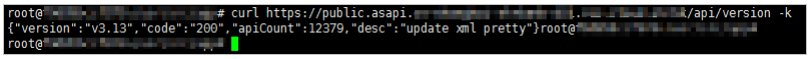
Verify an endpoint

Enter the following code. If you cannot access the endpoint, the endpoint is unavailable. You can use the historical endpoint.

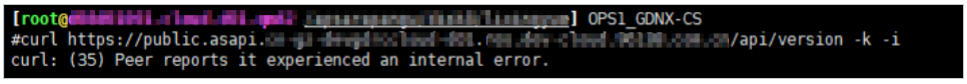
```
curl https://public.asapi.${global:region}.${global:internet-domain}/api/version -k
```

> **Note**
>
> `${global:region}` and `${global:internet-domain}` are variables. You must replace them with the actual values that you obtained.

Sample available endpoint:



Sample unavailable endpoint:



Historical endpoint

Only the HTTP protocol is supported. The historical endpoint is suffixed with `intranet-domain` and in the following format:

```
http://server.asapi.${global:region}.${global:intranet-domain}/asapi/v3
```

> **Note**
>
> `${global:region}` and `${global:intranet-domain}` are variables. You must replace them with the actual values that you obtained.

Procedure

To obtain the actual values of the variables ${global:region}, ${global:internet-domain}, and ${global:intranet-domain}, perform the following steps:

1. In the address bar, enter the *region-id*.aso.*intranet-domain-id*.com URL and press the Enter key.

   > **Note**
   >
   > You can select a language from the drop-down list in the upper-right corner of the page.

2. Enter your username and password.

   > **Note**
   >
   > Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from deployment engineers or an administrator.

   If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   To enhance security, make sure that the password meets the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password is 10 to 20 characters in length.

3. Click **Log On** to log on to the Apsara Uni-manager Operations Console. In the top navigation bar, choose **Products** > **Platforms** > **Apsara Infrastructure Management Framework**.
4. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
5. On the **Clusters Operations** page, enter **ascm-A** in the **Cluster** search box to find the cluster. Click the cluster name.
6. On the **Cluster Details** page, click the **Cluster Configuration** tab.
7. In the left-side file list on the **Cluster Configuration** tab, click **kv.conf**.

   Replace `${global:region}` with the obtained region value, `${global:internet-domain}` with the obtained internet-domain value, and `${global:intranet-domain}` with the obtained intranet-domain value.

   > **Note**
   >
   > `${global:}` is not included in the endpoint of ASAPI that you can use.

7.2.2. Obtain the ASAPI SDK

Apsara Stack API (ASAPI) is a unified portal provided by Apsara Stack. You can use ASAPI to connect to all Apsara Stack services. Apsara Stack provides SDKs for API calls.

Public environment

If you use the public environment, you can go to the Apsara Stack documentation page and download the ASAPI SDK in the **Other Resources** section at the lower part of the page.

Private environment

If you use the private environment, you must switch to the public environment and then go to the Apsara Stack documentation page. At the lower part of the page, download the ASAPI SDK in the **Other Resources** section.

ASAPI SDK for Java

greopId	artifactId	version
com.alibaba	alicrypto-java-aliyun	1.0.4

groupId	artifactId	version
com.alibaba	fastjson	1.2.68
org.bouncycastle	bcprov-jdk15to18	1.66
org.bouncycastle	bcpkix-jdk15on	1.65
org.bouncycastle	bcprov-jdk15on	1.65
com.aliyun	gmsse	1.1.0
org.apache.commons	commons-lang3	3.0
commons-codec	commons-codec	1.11
commons-logging	commons-logging	1.2
org.apache.httpcomponents	httpcore	4.4.11
org.apache.httpcomponents	httpclient	4.5.7

ASAPI SDK for Python

Package	Version
aliyun-python-sdk-core	2.13.35
certifi	2021.5.30
cffi	1.14.6
charset-normalizer	2.0.4
cryptography	3.4.8
idna	3.2
jmespath	0.10.0
pycparser	2.20
requests	2.26.0
urllib3	1.26.6

Note You can use the version for each package listed in the preceding table or a later version.

7.3. STS overview

7.3.1. What is STS?

Apsara Stack Security Token Service (STS) allows you to manage temporary credentials to your Apsara Stack resources. Resource Access Management (RAM) provides RAM users and roles. A RAM role does not have permanent identity credentials. A RAM role can be assumed for Apsara Stack resource access only by using an STS token. When an STS token is issued, you can specify a validity period and access permissions for the STS token.

Use an STS token to assume a RAM role

An authorized RAM user can use an AccessKey pair to call the AssumeRole operation. This way, the RAM user can obtain an STS token of a RAM role and use the STS token to access Apsara Stack resources.

Benefits

- STS tokens reduce the risks of AccessKey pair leaks. An AccessKey pair is a long-term credential for a RAM user.
- STS tokens are temporary credentials. You can specify a validity period for an STS token. The token automatically becomes invalid when it expires. You do not need to rotate STS tokens on a regular basis.
- You can attach custom policies to STS tokens for flexible and fine-grained authorization.

7.3.2. AssumeRole

Obtains a Security Token Service (STS) token that is used by a RAM user to assume a RAM role. In this example, an Apsara Stack tenant account is used as the trusted entity of the RAM role.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AssumeRole	The operation that you want to perform. Set the value to AssumeRole.

Parameter	Type	Required	Example	Description
RoleArn	String	Yes	acs:ram::123456789012****:role/adminrole	The Apsara Stack Resource Name (ARN) of the RAM role. The trusted entity of the RAM role is an Apsara Stack tenant account.
RoleSessionName	String	Yes	alice	The name of the role session. Set this parameter based on your business requirements. In most cases, you can set this parameter to the identity of the user who calls the operation. For example, specify a username. In ActionTrail logs, you can distinguish the users who assume the same RAM role to perform operations based on the value of the **RoleSessionName** parameter. This way, you can perform user-specific auditing. The name must be 2 to 64 characters in length and can contain letters, digits, periods (.), at signs (@), hyphens (-), and underscores (_).
Policy	String	No	{"Statement": [{"Action": ["*"],"Effect": "Allow","Resource": ["*"]}],"Version":"1"}	The policy that specifies the permissions of the STS token. You can use this parameter to grant the STS token fewer permissions than the permissions granted to the RAM role. The policy must be 1 to 1,024 characters in length.

Responses

Parameter	Type	Example	Description
RequestId	String	6894B13B-6D71-4EF5-88FA-F32781734A7F	The ID of the request.
Credentials	None	None	The access credentials.
AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	The AccessKey ID.
AccessKeySecret	String	wyLTSmsyPGP1ohvvw8xYgB29dlGI8KMiH2pK****	The AccessKey secret.
SecurityToken	String	********	The security token.
Expiration	String	2015-04-09T11:52:19Z	The time when the STS token expires.
AssumedRoleUser	None	None	The temporary identity that you use to assume the RAM role.
Arn	String	acs:ram::123456789012****:role/adminrole/alice	The ARN of the temporary identity that you use to assume the RAM role.
AssumedRoleId	String	34458433936495****:alice	The ID of the temporary identity that you use to assume the RAM role.

Examples

Add Project Object Model (POM) dependencies

The Alibaba Cloud core library is required. Perform the following steps to add the Alibaba Cloud core library to POM:

```
<dependency>
  <groupId>com.aliyun</groupId>
  <artifactId>aliyun-java-sdk-core</artifactId>
  <version>[4.4.9,5.0.0)</version>
</dependency>
```

Call an API operation to obtain the STS AccessKey 3-tuple.

In the following sample code, the `Sts::AssumeRole::2015-04-01` operation is used to obtain the 3-tuple.

```
package com.aliyuns.test;

import com.alibaba.fastjson.JSONObject;
import com.aliyuncs.CommonRequest;
import com.aliyuncs.CommonResponse;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.http.FormatType;
import com.aliyuncs.http.HttpClientConfig;
import com.aliyuncs.http.MethodType;
import com.aliyuncs.http.ProtocolType;
import com.aliyuncs.profile.DefaultProfile;
import org.apache.commons.lang3.StringUtils;

public class STSAccessKeyDemo {
    public static void main(String[] args) {
        // Create and initialize a DefaultAcsClient instance.
        DefaultProfile profile = DefaultProfile.getProfile("<yourRegionID>", "<yourAccessKeyID>", "<yourAccessKeySecret>");
        HttpClientConfig clientConfig = HttpClientConfig.getDefault();
        clientConfig.setIgnoreSSLCerts(true);
        clientConfig.setProtocolType(ProtocolType.HTTPS);
        profile.setHttpClientConfig(clientConfig);
        IAcsClient client = new DefaultAcsClient(profile);
        CommonRequest request = new CommonRequest();
        // Replace "sts.aliyuns.com" with the actual endpoint of STS. In most cases, the endpoint is in the following format: sts-vpc.${global:region
}.${global:internet-domain}.
        request.setSysDomain("sts.aliyuns.com");
        request.setSysProduct("Sts");
        request.setSysAction("AssumeRole");
        request.setSysVersion("2015-04-01");
        request.setSysMethod(MethodType.POST);
        request.setHttpContentType(FormatType.FORM);
        // Replace "<yourRoleSessionName>" with the alias that you specify for the current role session.
        request.putQueryParameter("RoleSessionName", "<yourRoleSessionName>");
        // Replace "<yourRoleArn>" with the actual ARN that you obtained for the RAM role in the preceding step.
        request.putQueryParameter("RoleArn", "<yourRoleArn>");
        try {
            CommonResponse response = client.getCommonResponse(request);
            String assumeRole = response.getData();
            if (StringUtils.isEmpty(assumeRole)) return;
            JSONObject assumeRoleJson = JSONObject.parseObject(assumeRole);
            JSONObject credentials = assumeRoleJson.getJSONObject("Credentials");
            // Obtain the STS AccessKey 3-tuple.
            String stsAK = credentials.getString("AccessKeyId");
            String stsSK = credentials.getString("AccessKeySecret");
            String stsToken = credentials.getString("SecurityToken");
            System.out.println("stsAk: " + stsAK +"\nstsSk: " + stsSK + "\nstsToken: " + stsToken);
        } catch (ServerException e) {
            System.out.println(e.getErrCode());
            System.out.println(e.getErrMsg());
        } catch (ClientException e) {
            System.out.println(e.getErrCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

Call examples

In the following sample code, the `DescribeZones` operation in Elastic Compute Service (ECS) is used.

```
package com.aliyuns.test;

import com.aliyuncs.CommonRequest;
import com.aliyuncs.CommonResponse;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.http.FormatType;
import com.aliyuncs.http.HttpClientConfig;
import com.aliyuncs.http.MethodType;
import com.aliyuncs.http.ProtocolType;
import com.aliyuncs.profile.DefaultProfile;

public class DescribeZonesDemo {
    public static void main(String[] args) {
        // Replace "<yourRegionID>" with the actual region ID.
        // Replace "<yourStsAccesskey>" and "<yourStsAccessKeySecret>" with the AccessKey ID and secret in the 3-tuple that you obtained in the prece
ding step.
        DefaultProfile profile = DefaultProfile.getProfile("<yourRegionID>", "<yourStsAccessKey>", "<yourStsAccessKeySecret>");
        HttpClientConfig clientConfig = HttpClientConfig.getDefault();
        clientConfig.setIgnoreSSLCerts(true);
        clientConfig.setProtocolType(ProtocolType.HTTPS);
        profile.setHttpClientConfig(clientConfig);
        IAcsClient client = new DefaultAcsClient(profile);
        CommonRequest request = new CommonRequest();
        request.setSysDomain("ecs.aliyuns.com");
        request.setSysProduct("Ecs");
        request.setSysAction("DescribeZones");
        request.setSysVersion("2014-05-26");
        request.setSysMethod(MethodType.POST);
        request.setHttpContentType(FormatType.FORM);
        //Replace "<yourRegionID>" with the actual region ID.
        request.putHeadParameter("x-acs-regionid", "<yourRegionID>");
        // Replace "<yourStsToken>" with the STS token in the 3-tuple that you obtained in the preceding step.
        request.putQueryParameter("SecurityToken", "<yourStsToken>");
        // Optional. Specify the resource set ID.
        // request.putHeadParameter("x-acs-resourcegroupid", "<yourResourceGroupID>");
        // Required. Specify the organization ID.
        request.putHeadParameter("x-acs-organizationid", "<yourOrganizationID>");
        try {
            CommonResponse response = client.getCommonResponse(request);
            System.out.println(response.getData());
        } catch (ServerException e) {
            System.out.println(e.getErrCode());
            System.out.println(e.getErrMsg());
        } catch (ClientException e) {
            System.out.println(e.getErrCode());
            System.out.println(e.getErrMsg());
        }
    }
}
```

Error codes

HttpCode	Error code	Error message	Description
400	InvalidParameter	The parameter RoleArn is wrongly formed.	The error message returned because the ARN format of the RAM role is invalid.
400	InvalidParameter.RoleArn	The parameter RoleArn is wrongly formed.	The error message returned because the ARN format of the RAM role is invalid.
400	InvalidParameter.RoleSessionName	The parameter RoleSessionName is wrongly formed.	The error message returned because the value of the **RoleSessionName** parameter is in an invalid format. The value must be 2 to 64 characters in length and can contain letters, digits, periods (.), at signs (@), hyphens (-), and underscores (_).
400	InvalidParameter.DurationSeconds	The Min/Max value of DurationSeconds is 15min/1hr.	The error message returned because the value of the **DurationSeconds** parameter is invalid. The minimum value is 900, and the maximum value is equal to the value of the **MaxSessionDuration** parameter.
400	InvalidParameter.PolicyGrammar	The parameter Policy has not passed grammar check.	The error message returned because the syntax of the policy is invalid.

HttpCode	Error code	Error message	Description
400	InvalidParameter.PolicySize	The size of Policy must be smaller than 1024 bytes.	The error message returned because the length of the specified policy string exceeds the upper limit. The policy string can be up to 1,024 characters in length.
403	NoPermission	You are not authorized to do this action. You should be authorized by RAM.	The error message returned because the STS token does not have the required permissions.
404	EntityNotExist.Role	The specified Role not exists.	The error message returned because the specified RAM role does not exist.
500	InternalError	STS Server Internal Error happened.	The error message returned because an internal server error occurred.