

Alibaba Cloud

Apsara Stack Enterprise

VPN Gateway Developer Guide

Product Version: v3.16.2

Document Version: 20220913

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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Getting started	08
1.1. Usage notes on development documentation	08
1.2. Call an API operation	08
2. Preparations	09
2.1. Log on to the API Tool console	09
2.2. Obtain API information	09
2.3. Obtain an AccessKey pair	09
2.4. Obtain an STS AccessKey 3-tuple	10
2.5. Obtain the values of common header parameters	12
2.6. Obtain the endpoint of VPN Gateway	13
2.7. Obtain a VPN Gateway SDK	13
3. Call examples for SDK for Java	15
3.1. Getting started	15
3.2. Use SDK	16
3.2.1. Install VPC SDK for Java	16
3.2.2. Configure authentication credentials	16
3.2.3. Configure connection requests	17
3.2.4. Initiate a request	17
3.2.5. Troubleshooting	18
3.2.6. Use CommonRequest to call API operations	18
4. Call examples for SDK for Python	20
4.1. Getting started	20
4.2. Use SDK	20
4.2.1. Install VPC SDK for Python	20
4.2.2. Configure authentication credentials	21
4.2.3. Set HTTPS requests	21

4.2.4. Initiate a request	21
4.2.5. Handle errors	22
4.2.6. Use CommonRequest to call API operations	22
5.Call examples for SDK for Go	24
5.1. Quick start	24
5.2. Use SDK	24
5.2.1. Install the core package of SDK for Go	24
5.2.2. Configure authentication credentials	25
5.2.3. Initiate a request	25
5.2.4. Handle errors	25
5.2.5. Use CommonRequest to call API operations	26
6.API reference	28
6.1. List of operations by function	28
6.2. Make API requests	29
6.2.1. Request syntax	29
6.2.2. API authorization	29
6.2.3. Request signatures	29
6.2.4. RAM authentication	30
6.2.5. Common parameters	31
6.3. VPN gateway	32
6.3.1. CreateVpnGateway	32
6.3.2. ModifyVpnGatewayAttribute	33
6.3.3. DescribeVpnGateways	34
6.3.4. DescribeVpnGateway	37
6.3.5. DeleteVpnGateway	38
6.3.6. DescribeRegions	39
6.4. Customer gateway	40
6.4.1. CreateCustomerGateway	40

6.4.2. ModifyCustomerGatewayAttribute	42
6.4.3. DescribeCustomerGateways	43
6.4.4. DescribeCustomerGateway	45
6.4.5. DeleteCustomerGateway	46
6.5. Routes for VPN gateways	47
6.5.1. CreateVpnRouteEntry	47
6.5.2. ModifyVpnRouteEntryWeight	49
6.5.3. DeleteVpnRouteEntry	50
6.5.4. DescribeVpnRouteEntries	52
6.5.5. PublishVpnRouteEntry	53
6.5.6. CreateVpnPbrRouteEntry	55
6.5.7. ModifyVpnPbrRouteEntryWeight	57
6.5.8. DeleteVpnPbrRouteEntry	58
6.5.9. DescribeVpnPbrRouteEntries	59
6.6. IPsec-VPN	61
6.6.1. CreateVpnConnection	61
6.6.2. ModifyVpnConnectionAttribute	64
6.6.3. DescribeVpnConnections	68
6.6.4. DescribeVpnConnection	72
6.6.5. DownloadVpnConnectionConfig	75
6.6.6. DeleteVpnConnection	77
6.7. SSL-VPN	78
6.7.1. CreateSslVpnServer	78
6.7.2. ModifySslVpnServer	80
6.7.3. DescribeSslVpnServers	83
6.7.4. DescribeVpnSslServerLogs	85
6.7.5. DeleteSslVpnServer	86
6.7.6. CreateSslVpnClientCert	87

6.7.7. ModifySslVpnClientCert	88
6.7.8. DescribeSslVpnClientCerts	89
6.7.9. DescribeSslVpnClientCert	91
6.7.10. DeleteSslVpnClientCert	93
7.Appendixes	95
7.1. Use the ASAPI gateway to call API operations	95
7.2. Use the ASAPI gateway to make API calls	96
7.2.1. Obtain the endpoint of ASAPI	96
7.2.2. Obtain the ASAPI SDK	98
7.3. STS overview	99
7.3.1. What is STS?	99
7.3.2. AssumeRole	99

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 point of presence (POP) gateway or the Apsara Stack API (ASAPI) gateway. To ensure that Apsara Stack provi

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](#), and

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 pair](#) or [Obtain STS AccessKey credentials](#).

Note

We recommend that you use an AccessKey pair or STS AccessKey credentials of a personal account 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 organization to which the current user belongs is queried.
- If you do not set the `<x-acs-resourcegroupid>` parameter, this parameter is left empty by default. If you specify a resource set, you must also specify an organization ID.

4. Obtain the API references.

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 information, see the developer guide of the cloud service.

5. Obtain the cloud service endpoint.

6. Obtain the cloud service SDK 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 an AccessKey pair

AccessKey credentials are provided 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 provided by RAM.

Context

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

AccessKey credentials can be provided by RAM or STS:

- An AccessKey pair that is provided by RAM to a third party consists of an AccessKey ID and an AccessKey secret.
- An AccessKey 3-tuple that is provided 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	Description
x-acsc-regionid	The ID of the region. Example: <i>cn-hangzhou-*</i> .
x-acsc-organizationid	The ID of the organization in the Apsara Uni-manager Management Console. For more information about how to obtain organization IDs, see the <i>GetOrganizationList</i> section in <i>Apsara Uni-manager Management Console Developer Guide</i> .
x-acsc-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 <i>ListResourceGroup</i> section in <i>Apsara Uni-manager Management Console Developer Guide</i> .
x-acsc-instanceid	The ID of the instance that you want to manage. You can obtain instance IDs from the instance list.

Obtain the AccessKey pair of a personal account

1. Log on to the [Apsara Uni-manager Management Console](#).
2. In the upper-right corner of the homepage, move the pointer over the profile picture and click **User Information**.
3. In the **AccessKey Pair** section, view the AccessKey pair of your account.

AccessKey Pair [Create AccessKey Pair](#)

The AccessKey pair including the AccessKey ID and AccessKey secret is the credential for you to use Apsara Stack resources with full permissions. You must keep the AccessKey pair confidential.

AccessKey ID	AccessKey Secret	Status	Created At	Actions
C2cPgkKxP7-*		Enable	Jan 06, 2022, 09:10:51	Disable Delete

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

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**.
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 variable parameters with your actual information. Delete the angle brackets (<>) in the final code.

The following section describes the variable 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 and initialize a DefaultAcsClient instance.
    // 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 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 STS endpoint. The general format 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 RAM role ARN that is obtained in the previous step.
    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

`DescribeCustomerGateway` operation of VPN Gateway.

Note

In the following code, replace the variable parameters with your actual information. Delete the angle brackets (<>) in the final code.

The following section describes the variable 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 previous 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.aliyuncs.com");
    request.setSysProduct("Vpc");
    request.setSysAction("DescribeCustomerGateway");
    request.setSysVersion("2016-04-28");
    request.setSysMethod(MethodType.POST);
    request.setHttpContentType(FormatType.FORM);
    // Replace "<yourRegionID>" with the region ID.
    request.putHeadParameter("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.putHeadParameter("x-acs-resourcegroupid", "<yourResourceGroupID>");
    // Required. Replace the parameter with 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());
    }
}
```

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 ID of the region. For more information about how to obtain region IDs, see Obtain a region ID .
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 Obtain an organization ID .
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 Obtain a resource set ID .
x-acs-instanceid	The ID of the instance on which you want to perform operations. For more information about how to obtain instance IDs, 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 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*.

Obtain a resource set ID

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*.

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 VPN 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, choose **VPN > VPN Gateways**.
4. View the **IDs** and **names** of VPN gateways on the **VPN gateway** page.

Response parameters

The following response parameters are returned by default when you call API 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 endpoint of VPN Gateway

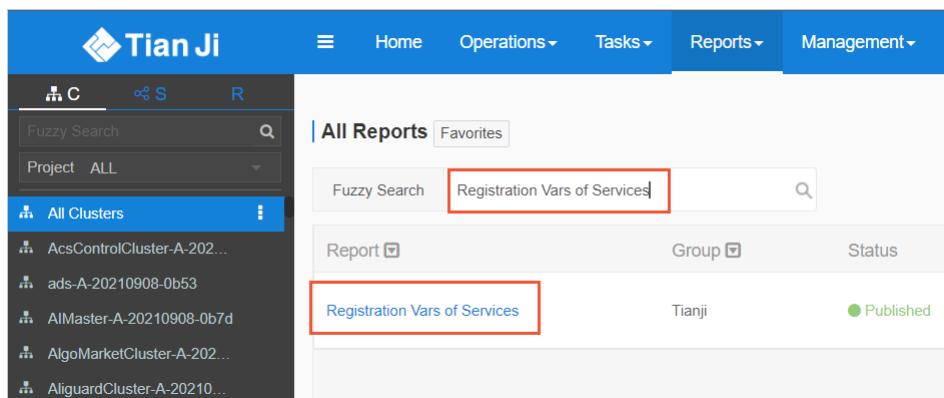
This topic describes how to obtain the endpoint of VPN Gateway.

Background information

To use the POP gateway to call API operations in Apsara Stack, you must specify the endpoint of a cloud service. You can obtain an endpoint from onsite Apsara Stack O&M engineers. You can also perform the following operations to obtain an endpoint.

Procedure

1. Log on to the Apsara Infrastructure Management console.
 - i. Log on to the Apsara Uni-manager Operations Console.
 - ii. In the top navigation bar, click **Products**.
 - iii. Choose **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`. In the report list that appears, click the name of the report.



4. On the **Registration Vars of Services** page, click the icon next to **Service** and search for `VPC`.
5. Find `vpc-yaochi`. Right-click the value in the **Service Registration** column and select **Show More**.

In the **Details** dialog box, view the value of `vpc-internal.openapi.endpoint`. This value indicates the `endpoint` of VPN Gateway.

2.7. Obtain a VPN Gateway SDK

When you call API operations in Apsara Stack by using the point of presence (POP) gateway, you must use an SDK of your cloud service. This topic describes how to obtain Apsara Stack SDKs.

An SDK includes code and examples. You can create cloud applications by using an SDK in the programming language that you require.

Background information

To use VPN gateways, you must install a virtual private cloud (VPC) SDK and the Apsara Stack core library. For example, to use VPC SDK for Java, you must download

```
aliyun-java-sdk-vpc and aliyun-java-sdk-core .
```

- A 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. An Apsara Stack 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 applicable to all cloud services and is compatible with Apsara Stack.

Obtain VPC SDKs

The SDKs for Java, Python, and Go are provided. You can obtain the SDKs from [Apsara Stack SDKs](#) based on your business requirements.

Note

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

3.Call examples for SDK for Java

3.1. Getting started

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

Prerequisites

- An authorized account and an AccessKey pair are obtained. The AccessKey pair consists of an AccessKey ID and an AccessKey secret. For more information, see [Obtain an AccessKey pair](#).
- The endpoint of VPN Gateway is obtained. For more information, see [Obtain the endpoint of VPN Gateway](#).
- SDKs for Java provided by Apsara Stack require Java Development Kit (JDK) 1.8 or later.

Install VPC SDK for Java

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

To use a VPC SDK, you must install the SDK core library and the VPC SDK. We recommend that you use version 4.5.17 or later for the SDK core library. In this example, the VPC SDK uses 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 variable parameters with your actual information. Delete the angle brackets (<>) in the final code.

The following section describes the variable 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 and initialize a DefaultAcsClient 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 current service. Replace the variable parameter with the endpoint.
        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 set the request parameters.
        DescribeCustomerGatewayRequest request = new DescribeCustomerGatewayRequest();
        // Configure service-related parameters.
        request.setCustomerGatewayId("<yourInstanceID>");
        // Specify the organization ID and resource set ID to query specified resources.
        request.putHeaderParameter("x-acs-organizationid", "apstrea****");
        request.putHeaderParameter("x-acs-resourcegroupid", "rs-1018fc75f29c0aab491e****");
        // Send the request and handle the response or exception.
        DescribeCustomerGatewayResponse response;
        try {
            DescribeCustomerGatewayResponse 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. The features of VPN Gateway are implemented by using VPC SDK for Java.

Apsara Stack SDK for Java supports Java Development Kit (JDK) 1.8 or later. You can install Apsara Stack SDK for Java by adding Maven dependencies or downloading [Apsara Stack SDK](#).

To use the development tool kit for VPC, you must install the core library of Apsara Stack SDK for Java and VPC SDK for Java. We recommend that you use the core library version 4.5.17 or later, and use Apsara Stack SDK for Java 3.2.0.

To use VPC SDK for Java, you must install the core library of Apsara Stack SDK for Java and add the following dependencies to the pom.xml file. For more information about the specific SDK version, see [Apsara Stack 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 Apsara Stack SDK to access Apsara Stack services, you must provide an Apsara Stack tenant account for authentication. This topic describes how to configure authentication credentials.

Apsara SDK for Java supports authentication through AccessKey pairs. For more information about how to obtain an AccessKey pair, see [Obtain an AccessKey pair](#).

If you use an AccessKey pair as the access credential, you must configure your credential when you initialize the client.

Note

Do not disclose code containing your AccessKey pair (for example, do not commit the code to public GitHub projects). Otherwise, your Apsara Stack tenant account may be compromised.

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

Note

In the preceding sample code, replace the variable parameters with the actual information. Remove the brackets (<>) in the final code.

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.

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 the API name, for example, `DescribeCustomerGateway`.

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

```
DescribeCustomerGatewayRequest request = new DescribeCustomerGatewayRequest();
// A customer gateway ID is used in the following example. Replace the ID with the actual ID of your customer gateway.
request.setCustomerGatewayId("cgw-ow25mqjb6mxnk*****");
// Special header parameters. Specify the organization ID and resource set ID. Resources are isolated.
request.putHeaderParameter("x-acs-organizationid", "appstrea*****");
request.putHeaderParameter("x-acs-resourcegroupid", "rs-1018fc75f29c0aab*****");
```

3. Initiate the request and handle the response.

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

In normal cases, all returned fields are deserialized into the response. You can directly use `response.getXXX()` to obtain the response fields.

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

If an exception occurs or you need 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.

Benefits

- **Lightweight:** You need to only download the core package. You do not need to download and install an SDK.
- **Easy to use:** You can call the newly released API operations of a service without the need to update the SDK of the service.
- **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.
- **Operation information:** 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 DescribeCustomerGateway operation, you must use `request.setSysAction("DescribeCustomerGateway")` to specify the API operation when you initiate a CommonRequest request.

Example: Call an RPC API operation

The following code shows how to obtain information about a customer gateway by calling the DescribeCustomerGateway operation of VPN Gateway.

Note In the following code, replace the variable parameters with your actual information. Delete the angle brackets (<>) in the final code.

The following section describes the variable 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 and initialize a DefaultAcsClient 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.
        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 set the request 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("DescribeCustomerGateway");
        request.putQueryParameter("CustomerGatewayId", "cgw-ow25mqjb6mxnk****");//Optional. Set the service parameters.
        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 or 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 an STS AccessKey 3-tuple to call an API operation, you must add the SecurityToken field in the request parameters.
         * Format:
         * 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. Getting started

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

Prerequisites

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

Install VPC SDK for Python

1. Install the SDK core library.

- 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
```

2. Install the SDK.

The following commands show 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 the region ID, AccessKey ID, and AccessKey secret.
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 variable parameters with your actual information. Delete the angle brackets (<>) in the final code.

The following section describes the variable 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.

```
#!/usr/bin/env python
#coding=utf-8
from aliyunsdkcore import client
from aliyunsdkcore.profile import region_provider
from aliyunsdkvpc.request.v20160428 import DescribeCustomerGateways
# global config
region_id = '<yourRegionID>' # Specify the region ID.
access_key = '<yourAccessKeyID>' # Specify the AccessKey ID.
access_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, access_secret, region_id)
# setup request
request = DescribeCustomerGatewaysRequest.DescribeCustomerGatewaysRequest()
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 default value is print (response).
```

4.2. Use SDK

4.2.1. Install VPC SDK for Python

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

SDKs for Python of Apsara Stack support Python 2.6.x, 2.7.x, 3.x, and later versions. You can install an SDK for Python by using pip.

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

Install the SDK of the service. The following examples show 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
```

4.2.2. Configure authentication credentials

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

SDKs for Python support 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 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.

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

4.2.3. 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.
```

4.2.4. Initiate a request

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

Procedure

1. Import the VPC SDK.

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

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

4. Initiate the request and process the response.

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

4.2.5. 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.

```
aliyun_sdk_core.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()
```

4.2.6. 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.

Benefits

- Lightweight: You need to only download the core package. You do not need to download and install an SDK.
- Easy to use: You can call the newly released API operations of a service without the need to update the SDK of the service.
- 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.

- Operation information: the name of the API operation that you want to call.

You need to 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 DescribeCustomerGateways operation, you must use `request.set_action_name('DescribeCustomerGateways')` to specify the API operation when you initiate a CommonRequest request.

Example: Call an RPC API operation

The following code shows how to obtain information about customer gateways by calling the DescribeCustomerGateways operation of VPN Gateway:

 **Note** In the following code, replace the variable parameters with your actual information. Delete the angle brackets (<>) in the final code.

The following section describes the variable 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.

```
from aliyuncore.client import AcsClient
from aliyuncore.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('DescribeCustomerGateways')
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='DescribeCustomerGateways', 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')
##### Add service parameters
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 VPN 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 an AccessKey pair](#).
- The endpoint of VPN Gateway is obtained. For more information, see [Obtain the endpoint of VPN 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:

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

Use Alibaba Cloud SDK for Go

The following sample code shows you how to use Alibaba Cloud SDK for Go:

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

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.
- <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.CreateDescribeCustomerGatewaysRequest()
    // 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.DescribeCustomerGateways(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 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 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 for VPN Gateway.

```
// 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 code, replace the parameters with your actual information. Delete the angle brackets (<>) in the final 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 VPN Gateway, you must use VPC SDK.

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

1. Import VPC SDK for Go.

```
import github.com/alibabacloud-sdk-go/services/vpc
```

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

 **Note** In the following code, replace the parameters with your actual information. Delete the angle brackets (<>) in the final 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`.

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

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

4. Initiate a call.

```
response, err := vpcClient.DescribeCustomerGateways(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.DescribeCustomerGateways(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 the error message in a `ClientError` of VPN Gateway:

 **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.DescribeCustomerGateways(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 the error message in a server error and a response of VPN Gateway:

 **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.DescribeCustomerGateways(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 code shows how to obtain information about customer gateways by calling the `DescribeCustomerGateways` operation of VPN Gateway:

 **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.
- <ecs.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 = "DescribeCustomerGateways"
    // 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.
    Use the following method:
    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 Enterprise 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 modify, 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 tables list API operations that are available for use in VPN Gateway.

VPN gateways

API	Description
CreateVpnGateway	Creates a VPN gateway.
ModifyVpnGatewayAttribute	Modifies the name and description of a VPN gateway.
DescribeVpnGateways	Queries VPN gateways.
DescribeVpnGateway	Queries detailed information about a specified VPN gateway.
DeleteVpnGateway	Deletes a VPN gateway.
DescribeRegions	Queries available regions.

Customer gateways

API	Description
CreateCustomerGateway	Creates a customer gateway.
ModifyCustomerGatewayAttribute	Modifies the name and description of a customer gateway.
DescribeCustomerGateways	Queries customer gateways.
DescribeCustomerGateway	Queries detailed information about a customer gateway.
DeleteCustomerGateway	Deletes a specified customer gateway.

VPN gateway routes

API	Description
CreateVpnRouteEntry	Creates a destination-based route entry for a VPN gateway.
CreateVpnPbrRouteEntry	Creates a policy-based route entry for a VPN gateway.
PublishVpnRouteEntry	Advertises a route entry of a VPN gateway to a virtual private cloud (VPC).
DescribeVpnRouteEntries	Queries destination-based route entries of a VPN gateway.
DescribeVpnPbrRouteEntries	Queries policy-based route entries of a VPN gateway.
ModifyVpnRouteEntryWeight	Modifies the weight of a destination-based route entry for a VPN gateway.
ModifyVpnPbrRouteEntryWeight	Modifies the weight of a policy-based route entry for a VPN gateway.
DeleteVpnRouteEntry	Deletes a destination-based route entry of a VPN gateway.
DeleteVpnPbrRouteEntry	Deletes a policy-based route entry of a VPN gateway.

IPsec-VPN

API	Description
CreateVpnConnection	Creates an IPsec-VPN connection.
ModifyVpnConnectionAttribute	Modifies the configuration of an IPsec-VPN connection.
DescribeVpnConnections	Queries IPsec-VPN connections.
DescribeVpnConnection	Queries detailed information about an IPsec-VPN connection.
DownloadVpnConnectionConfig	Downloads the configuration of an IPsec-VPN connection.
DeleteVpnConnection	Deletes a specified IPsec-VPN connection.

SSL-VPN

API	Description
CreateSslVpnServer	Creates an SSL-VPN server.
ModifySslVpnServer	Modifies the configuration of an SSL-VPN server.
DescribeSslVpnServers	Queries SSL-VPN servers.

API	Description
DescribeVpnSslServerLogs	Queries the logs of an SSL-VPN server.
DeleteSslVpnServer	Deletes an SSL-VPN server.
CreateSslVpnClientCert	Creates an SSL-VPN client certificate.
ModifySslVpnClientCert	Modifies the name of an SSL-VPN client certificate.
DescribeSslVpnClientCerts	Queries SSL-VPN client certificates.
DescribeSslVpnClientCert	Queries detailed information about an SSL-VPN client certificate.
DeleteSslVpnClientCert	Deletes an SSL-VPN client certificate.

6.2. Make API requests

6.2.1. Request syntax

To call a VPN Gateway API operation, you must send an HTTP GET request to the endpoint of the VPN Gateway API. 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.

VPN Gateway API operations use the RPC protocol. You can call VPN 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 API. The endpoint of the VPN Gateway API is `vpc.example.com`.

Note `example.com` is a custom domain name. You can obtain the endpoint in the Apsara Uni-manager Operations Console. For more information, see [Obtain the ASAPI endpoint](#).

- Action: the operation that you want to call. For example, you can call `DescribeVpnGateways` to query VPN gateways.
- Version: the version of the API that you want to call. The current version of the VPN Gateway API 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 shows how to call the `DescribeVpnGateways` operation to query VPN gateways.

Note The following code is formatted for ease of reading.

```
https://vpc.example.com/?Action=DescribeVpnGateways
&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 API operations as a Resource Access Management (RAM) user. Before you call the VPN Gateway API as a RAM user, you must create a RAM user and grant the RAM user the required permissions.

For more information about VPN resources and API operations that you can authorize a RAM user to use, see [RAM authentication](#).

6.2.3. Request signatures

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

VPN 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 Alibaba Cloud accounts and RAM users that is similar to a pair of 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 confidential. For more information about how to create an AccessKey pair, see [Obtain an AccessKey pair](#).

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
```

For example, you want to call the `DescribeVpcs` operation. The AccessKey ID is `testid` and the AccessKey secret is `testsecret`. The following code block shows the URL of the request before the request is signed

```
http://vpc.example.com/?Action=DescribeVpnGateways
&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 compose a string-to-sign.

```
GET%2F&AccessKeyId%3Dtestid&Action%3DDescribeVpnGateways&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamps%3D2016-02-23T12:46:24Z&Version%3D2016-04-28
```

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 as the Signature parameter.

```
http://vpc.example.com/?Action=DescribeVpnGateways
&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
```

6.2.4. RAM authentication

Before you call the VPN Gateway API as a RAM user, you must use an Apsara Stack tenant account to create a permission policy to assign permissions to the RAM user. In the permission policy, you must use an Alibaba Cloud Resource Name (ARN) to specify the resource that you want this RAM user to access.

Resources types of VPN Gateway that can be authorized

The following table lists the VPN Gateway resources that can be authorized and the ARNs of these resources.

Resource type	ARN
VPN gateway	<code>acs:vpc:\$regionid:\$accountid:vpngateway/\$vpngatewayid</code>
	<code>acs:vpc:\$regionid:\$accountid:vpngateway/*</code>
	<code>acs:vpc:*\$accountid:vpngateway/*</code>
Customer gateway	<code>acs:vpc:\$regionid:\$accountid:customergateway/\$customergatewayid</code>
	<code>acs:vpc:\$regionid:\$accountid:customergateway/*</code>
	<code>acs:vpc:*\$accountid:customergateway/*</code>
IPsec-VPN connection	<code>acs:vpc:\$regionid:\$accountid:vpnconnection/\$vpnconnectionid</code>
	<code>acs:vpc:\$regionid:\$accountid:vpnconnection/*</code>
	<code>acs:vpc:*\$accountid:vpnconnection/*</code>
SSL-VPN server	<code>acs:vpc:\$regionid:\$accountid:sslvpnserver/\$sslvpnserverid</code>
	<code>acs:vpc:\$regionid:\$accountid:sslvpnserver/*</code>
	<code>acs:vpc:*\$accountid:sslvpnserver/*</code>
SSL-VPN client certificate	<code>acs:vpc:\$regionid:\$accountid:sslvpnclientcert/\$sslvpnclientcertid</code>
	<code>acs:vpc:\$regionid:\$accountid:sslvpnclientcert/*</code>
	<code>acs:vpc:*\$accountid:sslvpnclientcert/*</code>
General-purpose resource	<code>acs:vpc:\$regionid:\$accountid:*</code>
	<code>acs:vpc:*\$accountid:*</code>

`$regionid`/`accountid`/`routerid` are the IDs of specific resources. `*` represents all resources.

VPN Gateway API operations that can be authorized

The following table lists the VPN Gateway API operations that can be authorized and the ARNs of these API operations.

API	ARN
ModifyVpnGatewayAttribute	acs:vpc:\$regionid:\$accountid:vpngateway/\$vpngatewayid
DescribeVpnGateways	acs:vpc:\$regionid:\$accountid:vpngateway/*
DescribeVpnGateway	acs:vpc:\$regionid:\$accountid:vpngateway/\$vpngatewayid
DeleteVpnGateway	acs:vpc:\$regionid:\$accountid:vpngateway/\$vpngatewayid
CreateCustomerGateway	acs:vpc:\$regionid:\$accountid:customergateway/*
DeleteCustomerGateway	acs:vpc:\$regionid:\$accountid:customergateway/\$customergatewayid
DescribeCustomerGateway	acs:vpc:\$regionid:\$accountid:customergateway/\$customergatewayid
DescribeCustomerGateways	acs:vpc:\$regionid:\$accountid:customergateway/*
ModifyCustomerGatewayAttribute	acs:vpc:\$regionid:\$accountid:customergateway/\$customergatewayid
CreateVpnConnection	acs:vpc:\$regionid:\$accountid:vpnconnection/*
DeleteVpnConnection	acs:vpc:\$regionid:\$accountid:vpnconnection/\$vpnconnectionid
DescribeVpnConnection	acs:vpc:\$regionid:\$accountid:vpnconnection/\$vpnconnectionid
DescribeVpnConnections	acs:vpc:\$regionid:\$accountid:vpnconnection/*
ModifyVpnConnectionAttribute	acs:vpc:\$regionid:\$accountid:vpnconnection/\$vpnconnectionid
DownloadVpnConnectionConfig	acs:vpc:\$regionid:\$accountid:vpnconnection/\$vpnconnectionid

6.2.5. Common parameters

Common parameters include common request parameters and common response parameters.

Common request parameters

Common request parameters must be included in all virtual private cloud (VPC) API requests. The following table describes the common request parameters.

Parameter	Type	Required	Description
Format	String	No	The format in which to return the response. Valid values: <i>JSON</i> and <i>XML</i> . Default value: <i>JSON</i> .
Version	String	Yes	The version number of the API. Format: <code>YYYY-MM-DD</code> . Valid values: <i>2016-04-28</i>
AccessKeyId	String	Yes	The AccessKey ID that is used to call VPC API operations.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to <i>HMAC-SHA1</i>
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the <code>yyyy-MM-ddTHH:mm:ssZ</code> format. The time must be in UTC. For example, you can use 2022-01-10T01:00:00Z to specify January 10, 2022, 09:00:00 (UTC+8).
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to <i>1.0</i>
SignatureNonce	String	Yes	A unique random number that is used to prevent replay attacks. You must use a unique random number for each request.

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 the JSON or XML format. The default response format is JSON. You can specify the response format when you call an operation.

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-->
<Operation name + Response>
  <!--Returned request tag-->
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
  <!--Returned data-->
</Operation name + Response>
```

- JSON format

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /*Returned data*/
}
```

6.3. VPN gateway

6.3.1. CreateVpnGateway

Creates a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateVpnGateway	The operation that you want to perform. Set the value to: CreateVpnGateway .
Bandwidth	Integer	Yes	5	The public bandwidth of the VPN gateway. Unit: Mbit/s. Valid values: 5, 10, 20, 50, and 100.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where you want to create the VPN gateway. You can call the DescribeRegions operation to query the most recent region list.
VpcId	String	Yes	vpc-bp1ub1yt9cvakoelj****	The ID of the virtual private cloud (VPC) where the VPN gateway is deployed.
EnableIpsec	Boolean	No	true	Specifies whether to enable the IPsec-VPN feature. Valid values: true: enables the IPsec-VPN feature. false: disables the IPsec-VPN feature. This is the default value.
EnableSsl	Boolean	No	true	Specifies whether to enable the SSL-VPN feature. Valid values: true: enables the SSL-VPN feature. false: disables the SSL-VPN feature. This is the default value.
Name	String	No	MYVPN	The name of the VPN gateway. The default value is the ID of the VPN gateway. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). The name must start with a letter, and cannot start with <code>http://</code> or <code>https://</code> .
SslConnections	Integer	No	5	The maximum number of concurrent connections. Valid values: 5, 10, and 20.
VSwitchId	String	No	vsw-bp1j5miw2bae9s2vt****	The ID of the vSwitch to which the VPN gateway belongs.

Response parameters

Parameter	Type	Example	Description
Name	String	myVpn	The name of the VPN gateway.
RequestId	String	54B48E3D-DF70-471B-AA93-08E683A1B457	The ID of the request.
VpnGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.

Examples

Sample requests

```
http(s)://vpc.example.com/?Action=CreateVpnGateway &Bandwidth=5 &RegionId=cn-qingdao-env66-d01 &VpcId=vpc-bp1ublyt9cvakoelj**** &
```

Sample success responses

XML format

```
<CreateVpnGatewayResponse>
  <Name>myVpn</Name>
  <VpnGatewayId>vpn-bp1q8bgx4xnkm2ogj****</VpnGatewayId>
  <RequestId>54B48E3D-DF70-471B-AA93-08E683A1B457</RequestId>
</CreateVpnGatewayResponse>
```

JSON format

```
{ "CreateVpnGatewayResponse": { "Name": "myVpn", "VpnGatewayId": "vpn-bp1q8bgx4xnkm2ogj****", "RequestId": "54B48E3D-DF70-471B-AA93-08E683A1B457" } }
```

6.3.2. ModifyVpnGatewayAttribute

Modifies the name and description of a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyVpnGatewayAttribute	The operation that you want to perform. Set the value to ModifyVpnGatewayAttribute .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the VPN gateway is created. You can call the DescribeRegions operation to query the most recent region list.
VpnGatewayId	String	Yes	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
Description	String	No	vpngateway	The description of the VPN gateway. The description must be 2 to 256 characters in length. It must start with a letter and cannot start with <code>http://</code> or <code>https://</code> .
Name	String	No	myvpn	The name of the VPN 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 <code>http://</code> or <code>https://</code> .

Response parameters

Parameter	Type	Example	Description
VpnGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.
VpcId	String	vpc-bp1ublyt9cvakoelj****	The ID of the virtual private cloud (VPC) to which the VPN gateway belongs.
VSwitchId	String	vsw-bp1y9ovl1cu9ou4tv****	The ID of the vSwitch to which the VPN gateway belongs.
InternetIp	String	116.XX.XX.69	The public IP address of the VPN gateway.
CreateTime	Long	1492753580000	The timestamp generated when the VPN gateway was created.
EndTime	Long	1495382400000	The timestamp to be generated when the VPN gateway expires.
Spec	String	5 Mbps	The specification of the VPN gateway.

Parameter	Type	Example	Description
Name	String	test	The name of the VPN gateway.
Description	String	test	The description of the VPN gateway.
Status	String	active	The status of the VPN gateway.
IntranetIp	String	172.XX.XX.104	The private IP address of the VPN gateway.
RequestId	String	54B48E3D-DF70-471B-AA93-08E683A1B457	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyVpnGatewayAttribute
&RegionId=cn-qingdao-env66-d01
&VpnGatewayId=vpn-bp1q8bgx4xnkm2ogj****
&<公共请求参数>
```

Sample success responses

XML format

```
<ModifyVpnGatewayAttributeResponse>
  <Name>aaa</Name>
  <Status>active</Status>
  <VpnGatewayId>vpn-bp1q8bgx4xnkm2ogj****</VpnGatewayId>
  <Spec>5M</Spec>
  <CreateTime>1492753580000</CreateTime>
  <IntranetIp>172.XX.XX.104</IntranetIp>
  <RequestId>54B48E3D-DF70-471B-AA93-08E683A1B457</RequestId>
  <InternetIp>116.XX.XX.69</InternetIp>
  <EndTime>1495382400000</EndTime>
  <VSwitchId>vsw-bp1y9ovl1cu9ou4tv****</VSwitchId>
  <VpcId>vpc-bp1ub1yt9cvakoelj****</VpcId>
</ModifyVpnGatewayAttributeResponse>
```

JSON format

```
{
  "Name": "aaa",
  "Status": "active",
  "VpnGatewayId": "vpn-bp1q8bgx4xnkm2ogj****",
  "Spec": "5M",
  "RequestId": "BA56EAF8-E3A9-4BE6-8511-8F03512153E2",
  "IntranetIp": "172.XX.XX.104",
  "CreateTime": "1492753580000",
  "InternetIp": "116.XX.XX.69",
  "EndTime": "1495382400000",
  "VSwitchId": "vsw-bp1y9ovl1cu9ou4tv****",
  "VpcId": "vpc-bp1ub1yt9cvakoelj****"
}
```

6.3.3. DescribeVpnGateways

Queries VPN gateways.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpnGateways	The operation that you want to perform. Set the value to DescribeVpnGateways .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the VPN gateway is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpcId	String	No	vpc-bp1ub1yt9cvakoelj****	The ID of the virtual private cloud (VPC) to which the VPN gateway belongs.
VpnGatewayId	String	No	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.

Parameter	Type	Required	Example	Description
Status	String	No	init	The status of the VPN gateway. Valid values: init: The VPN gateway is being initialized. provisioning: The VPN gateway is being prepared. active: The VPN gateway is running as expected. updating: The VPN gateway is being updated. Deleting: The VPN gateway is being deleted.
BusinessStatus	String	No	Normal	The payment status of the VPN gateway. Valid values: Normal: The VPN gateway does not have overdue payments and is running as expected. FinancialLocked: The VPN gateway is locked due to overdue payments.
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
VpnGateways	Array of VpnGateway		Detailed information about the VPN gateways.
VpnGateway			
VpnGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.
VpcId	String	vpc-bp1ub1yt9cvakoelj****	The ID of the VPC to which the VPN gateway belongs.
VSwitchId	String	vsw-bp1y9ovl1cu9ou4tv****	The ID of the vSwitch to which the VPN gateway belongs.
InternetIp	String	116.XX.XX.69	The public IP address of the VPN gateway.
CreateTime	Long	1515383700000	The timestamp generated when the VPN gateway was created.
EndTime	Long	1518105600000	The timestamp to be generated when the VPN gateway expires.
Spec	String	5 Mbps	The bandwidth limit of the VPN gateway.
Name	String	test	The name of the VPN gateway.
Description	String	test	The description of the VPN gateway.
Status	String	active	The status of the VPN gateway.
BusinessStatus	String	Normal	The payment status of the VPN gateway.
ChargeType	String	Prepay	The billing method of the VPN gateway. Valid value: PostpayByFlow .
IpssecVpn	String	enable	Indicates whether the IPsec-VPN feature is enabled. Valid values: enable: enabled disable: disabled
SslMaxConnections	Long	5	The maximum number of concurrent SSL-VPN connections.
SslVpn	String	enable	Indicates whether the SSL-VPN feature is enabled. Valid values: enable: enabled disable: disabled
Tag	String	1	The tag of the VPN gateway.

Parameter	Type	Example	Description
TotalCount	Integer	1	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	DF11D6F6-E35A-41C3-9B20-6FC8A901FE65	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVpnGateways
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVpnGatewaysResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <VpnGateways>
    <VpnGateway>
      <Status>active</Status>
      <VpnGatewayId>vpn-bp1q8bgx4xnm2ogj****</VpnGatewayId>
      <BusinessStatus>Normal</BusinessStatus>
      <Spec>5M</Spec>
      <CreateTime>1492753580000</CreateTime>
      <InternetIp>116.XX.XX.69</InternetIp>
      <EndTime>1495382400000</EndTime>
      <VSwitchId>vsw-bply9ovl1cu9ou4tv****</VSwitchId>
      <VpcId>vpc-bp1ublyt9cvakoel****</VpcId>
    </VpnGateway>
  </VpnGateways>
  <RequestId>DF11D6F6-E35A-41C3-9B20-6FC8A901FE65</RequestId>
</DescribeVpnGatewaysResponse>
```

JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "VpnGateways": {
    "VpnGateway": [
      {
        "Status": "active",
        "VpnGatewayId": "vpn-bp1q8bgx4xnm2ogj****",
        "BusinessStatus": "Normal",
        "Spec": "5M",
        "CreateTime": 1492753580000,
        "InternetIp": "116.XX.XX.69",
        "EndTime": 1495382400000,
        "VSwitchId": "vsw-bply9ovl1cu9ou4tv****",
        "VpcId": "vpc-bp1ublyt9cvakoel****"
      }
    ]
  },
  "PageSize": 10,
  "RequestId": "B2CD1315-CA2B-47B1-9DA5-8F1D69C48E82"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. Apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform this operation on the specified resource. To acquire the required permissions, submit a ticket.

6.3.4. DescribeVpnGateway

Queries the details of a specified VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpnGateway	The operation that you want to perform. Set the value to DescribeVpnGateway .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the VPN gateway is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnGatewayId	String	Yes	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.

Response parameters

Parameter	Type	Example	Description
VpnGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.
VpcId	String	vpc-bp1ub1yt9cvakoelj****	The ID of the VPC for which the VPN gateway is created.
VSwitchId	String	vsw-bp1y9ovl1cu9ou4tv****	The ID of the vSwitch to which the VPN gateway is attached.
InternetIp	String	116.XX.XX.222	The public IP address of the VPN gateway.
CreateTime	Long	1495382400000	The timestamp generated when the VPN gateway was created.
EndTime	Long	1495382400000	The timestamp to be generated when the VPN gateway expires.
Spec	String	5 M	The maximum bandwidth of the VPN gateway. Unit: Mbit/s.
Name	String	vpngatewayname	The name of the VPN gateway.
Description	String	vpngatewaydescription	The description of the VPN gateway.
Status	String	init	The status of the VPN gateway. init: The VPN gateway is being initialized. provisioning: The VPN gateway is being prepared. active: The VPN gateway is running as expected. updating: The VPN gateway is being updated. Deleting: The VPN gateway is being deleted.
BusinessStatus	String	Normal	The payment status of the VPN gateway. Normal: The VPN gateway is running as expected. FinancialLocked: The VPN gateway is locked due to overdue payments.
ChargeType	String	PostpayByFlow	The billing method of the VPN gateway. Valid value: PostpayByFlow .
IpssecVpn	String	enable	Indicates whether the IPsec-VPN feature is enabled. enable: IPsec-VPN is enabled. disable: IPsec-VPN is disabled.
RequestId	String	E98A9651-7098-40C7-8F85-C818D1EBBA85	The ID of the request.
SslMaxConnections	Long	5	The maximum number of concurrent SSL-VPN connections.
SslVpn	String	enable	Indicates whether the SSL-VPN feature is enabled. enable: SSL-VPN is enabled. disable: SSL-VPN is disabled.

Parameter	Type	Example	Description
Tag	String	tag1	The tag of the VPN gateway.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVpnGateway
&RegionId=cn-qingdao-env66-d01
&VpnGatewayId=vpn-bp1q8bgx4xnkm2ogj****
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVpnGatewayResponse>
  <Status>active</Status>
  <VpnGatewayId>vpn-bp1q8bgx4xnkm2ogj****</VpnGatewayId>
  <Spec>5M</Spec>
  <BusinessStatus>Normal</BusinessStatus>
  <RequestId>E98A9651-7098-40C7-8F85-C818D1EBBA85</RequestId>
  <CreateTime>1492753580000</CreateTime>
  <InternetIp>116.XX.XX.222</InternetIp>
  <EndTime>1495382400000</EndTime>
  <VSwitchId>vsw-bp1y9ovl1cu9ou4tv****</VSwitchId>
  <VpcId>vpc-bp1ublyt9cvakoelj****</VpcId>
</DescribeVpnGatewayResponse>
```

JSON format

```
{
  "Status": "active",
  "VpnGatewayId": "vpn-bp1q8bgx4xnkm2ogj****",
  "BusinessStatus": "Normal",
  "Spec": "5M",
  "CreateTime": 1492753580000,
  "RequestId": "E98A9651-7098-40C7-8F85-C818D1EBBA85",
  "InternetIp": "116.XX.XX.222",
  "EndTime": 1495382400000,
  "VSwitchId": "vsw-bp1y9ovl1cu9ou4tv****",
  "VpcId": "vpc-bp1ublyt9cvakoelj****"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.

6.3.5. DeleteVpnGateway

Deletes a specified VPN gateway.

 **Note** You cannot delete a VPN gateway that is associated with an IPsec-VPN connection.

Request parameters

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

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the VPN gateway is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnGatewayId	String	Yes	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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=DeleteVpnGateway
&RegionId=cn-qingdao-env66-d01
&VpnGatewayId=vpn-bp1q8bgx4xnkm2ogj****
&<Common request parameters>
```

Sample success responses

XML format

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

JSON format

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

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
403	ForbiddenRelease	Forbidden to release a prepaid instance within validity period	The error message returned because you cannot release a subscription VPN gateway within the subscription duration.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.Configuring	The specified VPN gateway is being configured.	The error message returned because the VPN gateway is being configured.

6.3.6. DescribeRegions

Queries the most recent region list.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRegions	The operation that you want to perform. Set the value to DescribeRegions .
ProductType	String	No	ECS	The type of the cloud service.
AcceptLanguage	String	No	zh-CN	The language of the response. Valid values: zh-CN: Chinese. This is the default value. en-US: English

Response parameters

Parameter	Type	Example	Description
Regions	Array of Region		The list of regions.
Region			
LocalName	String	China (Qingdao)	The name of the region.
RegionEndpoint	String	vpc.aliyuncs.com	The endpoint of the region.
RegionId	String	cn-qingdao-env17-d01	The ID of the region.
RequestId	String	611CB80C-B6A9-43DB-9E38-0B0AC3D9B58F	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeRegions
&<<Common request parameters>>
```

Sample success responses

XML format

```
<DescribeRegionsResponse>
  <RequestId>611CB80C-B6A9-43DB-9E38-0B0AC3D9B58F</RequestId>
  <Regions>
    <RegionId>cn-qingdao-env17-d01</RegionId>
    <RegionEndpoint>vpc.aliyuncs.com</RegionEndpoint>
    <LocalName>China (Qingdao)</LocalName>
  </Regions>
</DescribeRegionsResponse>
```

JSON format

```
{
  "RequestId": "611CB80C-B6A9-43DB-9E38-0B0AC3D9B58F",
  "Regions": {
    "RegionId": "cn-qingdao-env17-d01",
    "RegionEndpoint": "vpc.aliyuncs.com",
    "LocalName": "China (Qingdao)"
  }
}
```

6.4. Customer gateway

6.4.1. CreateCustomerGateway

Creates a customer gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateCustomerGateway	The operation that you want to perform. Set the value to CreateCustomerGateway .
IpAddress	String	Yes	116.XX.XX.222	The IP address of the customer gateway.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where you want to create the customer gateway. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token is used to ensure the idempotence of the request. You can use the client to generate a token, but you must make sure that the token is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.
Name	String	No	Gateway	The name of the customer 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. However, the name cannot start with <code>http://</code> or <code>https://</code> .
Description	String	No	Gateway	The description of the customer gateway. The description must be 2 to 256 characters in length, and contain digits, hyphens (-), underscores (_), full width periods (。), full width commas (，), and full width colons (：). The description cannot start with <code>http://</code> or <code>https://</code> .

Response parameters

Parameter	Type	Example	Description
CustomerGatewayId	String	cgw-bp1aw0a5nff03xp1****	The ID of the customer gateway.
IpAddress	String	100.XX.XX.1	The IP address of the customer gateway.
Name	String	test	The name of the customer gateway.
Description	String	test	The description of the customer gateway.
CreateTime	Long	1493363486000	The timestamp generated when the customer gateway was created.
RequestId	String	cgw-bp1aw0a5nff03xp1pcqc	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateCustomerGateway
&IpAddress=116.XX.XX.222
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<CreateCustomerGatewayResponse>
  <CustomerGatewayId>cgw-bp1aw0a5nff03xp1****</CustomerGatewayId>
  <RequestId>185E81B1-3916-4667-B48F-C52409B33F2B</RequestId>
  <CreateTime>1493363486000</CreateTime>
  <IpAddress>100.XX.XX.1</IpAddress>
</CreateCustomerGatewayResponse>
```

JSON format

```
{
  "CustomerGatewayId": "cgw-bp1jrawp82av6bws9****",
  "CreateTime": 1493363599000,
  "RequestId": "D32B3C26-6C6C-4988-93E9-D2A6444CE6AE",
  "IpAddress": "100.XX.XX.1"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	InvalidIpAddress.AlreadyExist	Specified IpAddress is already exist.	The error message returned because the specified IP address already exists. The IP addresses must be unique in the same region.
400	InvalidIpAddress.WrongFormat	Specified IpAddress is invalid.	The error message returned because the specified IP address is invalid.
400	InvalidName	The name is not valid	The error message returned because the specified name is in an invalid format.
400	InvalidDescription	The description is not valid	The error message returned because the description format of the specified parameter is invalid.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.

6.4.2. ModifyCustomerGatewayAttribute

Modifies the name and description of a customer gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyCustomerGatewayAttribute	The operation that you want to perform. Set the value to ModifyCustomerGatewayAttribute .
CustomerGatewayId	String	Yes	vpn-bp1q8bgx4xnkm2ogj****	The ID of the customer gateway.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the customer gateway is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	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.
Name	String	No	test	The name of the customer gateway. The name must be 2 to 128 characters in length, and can contain letters, digits, periods (.), underscores (_), and hyphens (-). The name must start with a letter. It cannot start with <code>http://</code> or <code>https://</code> .
Description	String	No	test	The description of the customer gateway. The description must be 2 to 256 characters in length and can contain digits, hyphens (-), underscores (_), periods (.), commas (,), and colons (:). The description must start with a letter, and cannot start with <code>http://</code> or <code>https://</code> .

Response parameters

Parameter	Type	Example	Description
CustomerGatewayId	String	cgw-bp1pvp19r9adju6l5****	The ID of the customer gateway.
Name	String	test	The name of the customer gateway.

Parameter	Type	Example	Description
Description	String	test	The description of the customer gateway.
IpAddress	String	139.XX.XX.55	The IP address of the customer gateway.
CreateTime	Long	1492747187000	The timestamp generated when the customer gateway was created.
RequestId	String	E61293C8-AF07-4E87-A272-542680038F93	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyCustomerGatewayAttribute
&CustomerGatewayId=vpn-bp1q8bgx4xnkm2ogj****
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyCustomerGatewayAttributeResponse>
  <CustomerGatewayId>cgw-bp1pvpl9r9adju6l5****</CustomerGatewayId>
  <RequestId>E61293C8-AF07-4E87-A272-542680038F93</RequestId>
  <CreateTime>1492747187000</CreateTime>
  <IpAddress>139.XX.XX.55</IpAddress>
  <Description>modify</Description>
</ModifyCustomerGatewayAttributeResponse>
```

JSON format

```
{
  "CustomerGatewayId": "cgw-bp1pvpl9r9adju6l5****",
  "RequestId": "8AA5CE21-2E6A-4530-BDF5-F055849476E6",
  "CreateTime": 1492747187000,
  "IpAddress": "139.XX.XX.55",
  "Description": "modify"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. Apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform this operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidCustomerGatewayInstanceId.NotFound	The specified customer gateway instance id does not exist.	The error message returned because the specified instance ID does not exist.
400	InvalidName	The name is not valid	The error message returned because the format of the name is invalid.
400	InvalidDescription	The description is not valid	The error message returned because the format of the description is invalid.

6.4.3. DescribeCustomerGateways

Queries customer gateways in a specified region.

Request parameters

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

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-qingdao-env66-d01	The region ID of the customer gateway. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
CustomerGatewayId	String	No	cgw-bp1pvpl9r9adju6l5****	The ID of the customer gateway.
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
CustomerGateways	Array of CustomerGateway		The details about the customer gateways.
CustomerGateway			
CustomerGatewayId	String	cgw-bp1pvpl9r9adju6l5****	The ID of the customer gateway.
Name	String	test	The name of the customer gateway.
Description	String	test	The description of the customer gateway.
IpAddress	String	139.XX.XX.55	The IP address of the customer gateway.
CreateTime	Long	1492747187000	The timestamp generated when the customer gateway was created.
TotalCount	Integer	1	The 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	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCustomerGateways
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeCustomerGatewaysResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>5BE01CD7-5A50-472D-AC14-CA181C5C03BE</RequestId>
  <CustomerGateways>
    <CustomerGateway>
      <Name>test</Name>
      <CustomerGatewayId>cgw-bp1pvpl9r9adju6l5****</CustomerGatewayId>
      <CreateTime>1492747187000</CreateTime>
      <IpAddress>139.XX.XX.55</IpAddress>
    </CustomerGateway>
  </CustomerGateways>
</DescribeCustomerGatewaysResponse>
```

JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "E82612A9-CB90-4D7E-B394-1DB7F6509B29",
  "CustomerGateways": {
    "CustomerGateway": [
      {
        "Name": "test",
        "CustomerGatewayId": "cgw-bp1pvpl9r9adju6l5****",
        "CreateTime": 1492747187000,
        "IpAddress": "139.XX.XX.55"
      }
    ]
  }
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. Acquire the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. Acquire the required permissions and try again.

6.4.4. DescribeCustomerGateway

Queries details of a specified customer gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCustomerGateway	The operation that you want to perform. Set the value to DescribeCustomerGateway .
CustomerGatewayId	String	Yes	cgw-bp1pvpl9r9adju6l5****	The ID of the customer gateway.
RegionId	String	Yes	cn-qingdao-env66-d01	The region ID of the customer gateway. You can call the <code>DescribeRegions</code> operation to query the most recent region list.

Response parameters

Parameter	Type	Example	Description
CustomerGatewayId	String	cgw-bp1pvpl9r9adju6l5****	The ID of the customer gateway.
Name	String	test	The name of the customer gateway.
Description	String	test	The description of the customer gateway.
IpAddress	String	139.XX.XX.32	The IP address of the customer gateway.
RequestId	String	99506ECB-218F-45A5-AE8E-79518451F615	The ID of the request.
CreateTime	Long	1492747187000	The timestamp generated when the customer gateway was created.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCustomerGateway
&CustomerGatewayId=vpn-bp1q8bgx4xnkm2ogj****
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeCustomerGatewayResponse>
  <Name>test</Name>
  <CustomerGatewayId>cgw-bp1pvpl9r9adju615****</CustomerGatewayId>
  <CreateTime>1492747187000</CreateTime>
  <RequestId>99506ECB-218F-45A5-AE8E-79518451F615</RequestId>
  <IpAddress>139.XX.XX.32</IpAddress>
</DescribeCustomerGatewayResponse>
```

JSON format

```
{
  "CustomerGatewayId": "cgw-bp1pvpl9r9adju615****",
  "Name": "test",
  "RequestId": "A0457BC9-6C0F-4437-AB9D-FB2EABC1D6A2",
  "CreateTime": 1492747187000,
  "IpAddress": "139.XX.XX.32"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. Acquire the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
404	InvalidCustomerGatewayInstanceId.NotFound	The specified customer gateway instance id does not exist.	The error message returned because the specified customer gateway does not exist. Check whether the ID of the customer gateway is valid.

6.4.5. DeleteCustomerGateway

Deletes a specified customer gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteCustomerGateway	The operation that you want to perform. Set the value to DeleteCustomerGateway .
CustomerGatewayId	String	Yes	cgw-2zllmw9lqrcdis3bd****	The ID of the customer gateway.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the customer gateway is created. You can call the DescribeRegions operation to query the most recent region list.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token is used to ensure the idempotence of the request. You can use the client to generate a token, but you must make sure that the token 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	606998F0-B94D-48FE-8316-ACAB1BB230DA	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteCustomerGateway
&CustomerGatewayId=vpn-bp1q8bgx4xnkm2ogj****
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<DeleteCustomerGatewayResponse>
  <RequestId>606998F0-B94D-48FE-8316-ACA81BB230DA</RequestId>
</DeleteCustomerGatewayResponse>
```

JSON format

```
{
  "RequestId": "606998F0-B94D-48FE-8316-ACA81BB230DA"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidCustomerGatewayInstanceId.NotFound	The specified customer gateway instance id does not exist.	The error message returned because the specified instance ID does not exist.

6.5. Routes for VPN gateways

6.5.1. CreateVpnRouteEntry

Creates a destination-based route on a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateVpnRouteEntry	The operation that you want to perform. Set the value to CreateVpnRouteEntry .
NextHop	String	Yes	vco-bp15oes1py4i66rmd****	The next hop of the destination-based route.
PublishVpc	Boolean	Yes	true	Specifies whether to advertise the destination-based route to the route table of the associated virtual private cloud (VPC). true: advertises the destination-based route to the route table of the associated VPC. false: does not advertise the destination-based route to the route table of the associated VPC.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the destination-based route is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
RouteDest	String	Yes	10.0.0.0/24	The destination CIDR block of the destination-based route.
VpnGatewayId	String	Yes	vpn-bp1a3kqjii9legfx****	The ID of the VPN gateway.
Weight	Integer	Yes	0	The weight of the destination-based route. Valid values: 0: specifies a low priority for the route. 100: specifies a high priority for the route.  Note If two destination-based route entries are configured with the same destination CIDR block, you cannot set the weights of both route entries to 100.
ClientToken	String	No	d7d24a21-f4ba-4454-9173-b3828dae492b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.

Parameter	Type	Required	Example	Description
Description	String	No	mytest	The description of the destination-based route.
OverlayMode	String	No	Ipsec	The overlay mode.

Response parameters

Parameter	Type	Example	Description
CreateTime	Long	1492747187000	The timestamp generated when the destination-based route was created.
Description	String	mytest	The description of the destination-based route.
NextHop	String	vco-bp15oes1py4i66rmd****	The next hop of the destination-based route.
OverlayMode	String	Ipsec	The overlay mode.
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.
RouteDest	String	10.0.0.0/24	The destination CIDR block of the destination-based route.
State	String	published	The status of the destination-based route. published: The route is advertised. normal: The route is not advertised.
VpnInstanceId	String	vpn-bp1cmw7jh1nfe43m9****	The ID of the VPN gateway.
Weight	Integer	0	The weight of the destination-based route. Valid values: 0 and 100 .

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateVpnRouteEntry
&NextHop=vco-bp15oes1py4i66rmd****
&PublishVpc=true
&RegionId=cn-qingdao-env66-d01
&RouteDest=10.0.0.0/24
&VpnGatewayId=vpn-bp1a3kqjiiq9legfx****
&Weight=0
&<Common request parameters>
```

Sample success responses

XML **format**

```
<CreateVpnRouteEntryResponse>
  <RouteDest>10.0.0.0/24</RouteDest>
  <VpnInstanceId>vpn-bp1cmw7jh1nfe43m9****</VpnInstanceId>
  <OverlayMode>Ipsec</OverlayMode>
  <State>published</State>
  <Weight>100</Weight>
  <CreateTime>1563873294331</CreateTime>
  <NextHop>vco-bp1tui07ob10fmuro****</NextHop>
  <RequestId>EE4C2417-9437-4333-BDEB-8493F7AA7258</RequestId>
</CreateVpnRouteEntryResponse>
```

JSON **format**

```
{
  "RouteDest": "10.0.0.0/24",
  "VpnInstanceId": "vpn-bp1cmw7jh1nfe43m9****",
  "OverlayMode": "Ipsec",
  "State": "published",
  "Weight": 100,
  "CreateTime": 1563873294331,
  "NextHop": "vco-bp1tui07ob10fmuro****",
  "RequestId": "CB2793A8-845F-444C-8E93-76F1BBDF9C78"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.5.2. ModifyVpnRouteEntryWeight

Modifies the weight of a destination-based route for a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyVpnRouteEntryWeight	The operation that you want to perform. Set the value to ModifyVpnRouteEntryWeight .
NewWeight	Integer	Yes	100	The new weight you want to set for the destination-based route. 0: specifies a low priority for the route entry. 100: specifies a high priority for the route entry.  Note If two destination-based route entries are configured with the same destination CIDR block, you cannot set the weights of both route entries to 100.
NextHop	String	Yes	vco-bp15oes1py4i66rmd****	The next hop of the destination-based route.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the destination-based route is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
RouteDest	String	Yes	10.0.0.0/24	The destination CIDR block of the destination-based route.
VpnGatewayId	String	Yes	vpn-bp1a3kqjiiq9legfx****	The ID of the VPN gateway.
Weight	Integer	Yes	0	The current weight of the destination-based route. Valid values: 0 and 100 .
ClientToken	String	No	d7d24a21-f4ba-4454-9173-b3828dae492b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
OverlayMode	String	No	Ipssec	The overlay mode. Set the value to Ipssec (IPsec tunneling).

Response parameters

Parameter	Type	Example	Description
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyVpnRouteEntryWeight
&NewWeight=100
&NextHop=vco-bp15oes1py4i66rmd****
&RegionId=cn-qingdao-env66-d01
&RouteDest=10.0.0/24
&VpnGatewayId=vpn-bp1a3kqjiiq9legfx****
&Weight=0
<<Common request parameters>
```

Sample success responses

XML format

```
<ModifyVpnRouteEntryWeightResponse>
  <RequestId>5BE01CD7-5A50-472D-AC14-CA181C5C03BE</RequestId>
</ModifyVpnRouteEntryWeightResponse>
```

JSON format

```
{
  "RequestId": "E82612A9-CB90-4D7E-B394-1DB7F6509B29"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.5.3. DeleteVpnRouteEntry

Deletes a destination-based route from a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteVpnRouteEntry	The operation that you want to perform. Set the value to DeleteVpnRouteEntry .
NextHop	String	Yes	vco-bp15oes1py4i66rmd****	The next hop of the destination-based route.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the destination-based route is created. You can call the DescribeRegions operation to query the most recent region list.
RouteDest	String	Yes	10.0.0/24	The destination CIDR block of the destination-based route.

Parameter	Type	Required	Example	Description
VpnGatewayId	String	Yes	vpn-bp1a3kqjiiq9legfx****	The ID of the VPN gateway.
Weight	Integer	Yes	0	The weight of the destination-based route. Valid values: 0: specifies a low priority for the route entry. 100: specifies a high priority for the route entry.  Note If two destination-based route entries are configured with the same destination CIDR block, you cannot set the weights of both route entries to 100.
ClientToken	String	No	d7d24a21-f4ba-4454-9173-b3828dae492b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
OverlayMode	String	No	Ipssec	The overlay mode. Set the value to Ipssec (IPsec tunneling).

Response parameters

Parameter	Type	Example	Description
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteVpnRouteEntry
&NextHop=vco-bp15oeslpy4i66rmd****
&RegionId=cn-qingdao-env66-d01
&RouteDest=10.0.0.0/24
&VpnGatewayId=vpn-bp1a3kqjiiq9legfx****
&Weight=0
<Common request parameters>
```

Sample success responses

XML format

```
<DeleteVpnRouteEntryResponse>
  <RequestId>5BE01CD7-5A50-472D-AC14-CA181C5C03BE</RequestId>
</DeleteVpnRouteEntryResponse>
```

JSON format

```
{
  "RequestId": "E82612A9-CB90-4D7E-B394-1DB7F6509B29"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.

HttpCode	Error code	Error message	Description
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.5.4. DescribeVpnRouteEntries

Queries destination-based routes of a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpnRouteEntries	The operation that you want to perform. Set the value to DescribeVpnRouteEntries .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the destination-based routes are created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnGatewayId	String	Yes	vpn-bp1a3kqjiiq9legfx****	The ID of the VPN gateway.
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
PageNumber	Integer	10	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	0ED8D006-F706-4D23-88ED-E11ED28DCAC0	The ID of the request.
TotalCount	Integer	10	The number of returned entries.
VpnRouteEntries	Array of VpnRouteEntry		The detailed information about the destination-based routes.
VpnRouteEntry			
CreateTime	Long	1492747187000	The timestamp generated when the destination-based route was created.
NextHop	String	vco-bp15oes1py4i66rmd****	The next hop of the destination-based route.
RouteDest	String	10.0.0.0/24	The destination CIDR block of the destination-based route.
State	String	published	The status of the destination-based route. published: The route is advertised. normal: The route is not advertised.
VpnInstanceId	String	vpn-bp1cmw7jh1nfe43m9****	The ID of the VPN gateway.
Weight	Integer	0	The weight of the destination-based route. Valid values: 0: indicates that the priority of the route entry is low. 100: indicates that the priority of the route entry is high.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVpnRouteEntries
&RegionId=cn-qingdao-env66-d01
&VpnGatewayId=vpn-bp1a3kqjiiq9legfx****
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVpnRouteEntriesResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <VpnRouteEntries>
    <VpnRouteEntry>
      <RouteDest>10.0.0.0/24</RouteDest>
      <VpnInstanceId>vpn-bp1cmw7jhlufe43m9****</VpnInstanceId>
      <State>normal</State>
      <Weight>100</Weight>
      <CreateTime>1563874074000</CreateTime>
      <NextHop>vco-bp1tui07ob10fmuro****</NextHop>
    </VpnRouteEntry>
  </VpnRouteEntries>
  <PageSize>10</PageSize>
  <RequestId>BF3995A6-FA4F-4C74-B90F-89ECF4BFF4D5</RequestId>
</DescribeVpnRouteEntriesResponse>
```

JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "VpnRouteEntries": {
    "VpnRouteEntry": [
      {
        "RouteDest": "10.0.0.0/24",
        "VpnInstanceId": "vpn-bp1cmw7jhlufe43m9****",
        "State": "normal",
        "Weight": 100,
        "CreateTime": 1563874074000,
        "NextHop": "vco-bp1tui07ob10fmuro****"
      }
    ]
  },
  "PageSize": 10,
  "RequestId": "BF3995A6-FA4F-4C74-B90F-89ECF4BFF4D5"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.

6.5.5. PublishVpnRouteEntry

Advertises a route of a VPN gateway to the route table of the associated virtual private cloud (VPC).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	PublishVpnRouteEntry	The operation that you want to perform. Set the value to PublishVpnRouteEntry .
NextHop	String	Yes	vco-bp15oes1py4i66rmd****	The next hop of the route.
PublishVpc	Boolean	Yes	true	Specifies whether to advertise the route of the VPN gateway to the route table of the associated VPC. true: advertises the route to the route table of the associated VPC. false: does not advertise the route to the route table of the associated VPC.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the route of the VPN gateway is deployed. You can call the <code>DescribeRegions</code> operation to query the most recent region list.

Parameter	Type	Required	Example	Description
RouteDest	String	Yes	10.0.0.0/24	The destination CIDR block of the route of the VPN gateway.
RouteType	String	Yes	pbr	The type of the route of the VPN gateway. Valid values: pbr: policy-based route. dbr: destination-based route.
VpnGatewayId	String	Yes	vpn-bp1a3kjiq9legfx****	The ID of the VPN gateway.
ClientToken	String	No	d7d24a21-f4ba-4454-9173-b3828dae492b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=PublishVpnRouteEntry
&NextHop=vco-bp15oes1py4i66rmd****
&PublishVpc=true
&RegionId=cn-qingdao-env66-d01
&RouteDest=10.0.0.0/24
&RouteType=pbr
&VpnGatewayId=vpn-bp1a3kjiq9legfx****
&<Common request parameters>
```

Sample success responses

XML **format**

```
<PublishVpnRouteEntryResponse>
  <RequestId>EE4C2417-9437-4333-BDEB-8493F7AA7258</RequestId>
</PublishVpnRouteEntryResponse>
```

JSON **format**

```
{
  "RequestId": "CB2793A8-845F-444C-8E93-76F1BBD9C78"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.5.6. CreateVpnPbrRouteEntry

Creates a policy-based route for a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateVpnPbrRouteEntry	The operation that you want to perform. Set the value to CreateVpnPbrRouteEntry .
NextHop	String	Yes	vco-bp15oes1py4i66rmd****	The next hop of the policy-based route.
PublishVpc	Boolean	Yes	true	Specifies whether to advertise the policy-based route to the route table of the associated virtual private cloud (VPC). Valid values: true: advertises the policy-based route to the route table of the associated VPC. false: does not advertise the policy-based route to the route table of the associated VPC.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where you want to create the policy-based route for the VPN gateway. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
RouteDest	String	Yes	10.0.0.0/24	The destination CIDR block of the policy-based route.
RouteSource	String	Yes	192.168.1.0/24	The source CIDR block of the policy-based route.
VpnGatewayId	String	Yes	vpn-bp1a3kqjiiq9legfx****	The ID of the VPN gateway.
Weight	Integer	Yes	0	The weight of the policy-based route. Valid values: 0: specifies a low priority for the route entry. 100: specifies a high priority for the route entry.  Note If two policy-based route entries are configured with the same destination CIDR block, you cannot set the weights of both route entries to 100.
ClientToken	String	No	d7d24a21-f4ba-4454-9173-b3828dae492b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
Description	String	No	vpnroute1	The description of the policy-based route.
OverlayMode	String	No	Ipsec	The overlay mode.

Response parameters

Parameter	Type	Example	Description
CreateTime	Long	1492747187000	The timestamp generated when the policy-based route was created.
Description	String	vpnroute1	The description of the policy-based route.
NextHop	String	vco-bp15oes1py4i66rmd****	The next hop of the policy-based route.
OverlayMode	String	Ipsec	The overlay mode.
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.
RouteDest	String	10.0.0.0/24	The destination CIDR block of the policy-based route.

Parameter	Type	Example	Description
RouteSource	String	192.168.1.0/24	The source CIDR block of the policy-based route.
State	String	normal	The status of the policy-based route. Valid values: published: The route is advertised. normal: The route is not advertised.
VpnInstanceId	String	vpn-bp1cmw7jh1nfe43m9****	The ID of the VPN gateway.
Weight	Integer	0	The weight of the policy-based route. Valid values: 0 and 100 .

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateVpnPbrRouteEntry
&NextHop=vco-bp15oes1py4i66rmd****
&PublishVpc=true
&RegionId=cn-qingdao-env66-d01
&RouteDest=10.0.0.0/24
&RouteSource=192.168.1.0/24
&VpnGatewayId=vpn-bp1a3kqjiiq9legfx****
&Weight=0
&<Common request parameters>
```

Sample success responses

XML **format**

```
<CreateVpnPbrRouteEntryResponse>
  <RouteDest>10.0.0.0/24</RouteDest>
  <RouteSource>192.168.1.0/24</RouteSource>
  <VpnInstanceId>vpn-bp1cmw7jh1nfe43m9****</VpnInstanceId>
  <OverlayMode>Ipsec</OverlayMode>
  <State>published</State>
  <Weight>100</Weight>
  <CreateTime>1563873294331</CreateTime>
  <NextHop>vco-bp1tui07ob10fmuro****</NextHop>
</CreateVpnPbrRouteEntryResponse>
```

JSON **format**

```
{
  "RouteDest": "10.0.0.0/24",
  "RouteSource": "192.168.1.0/24",
  "VpnInstanceId": "vpn-bp1cmw7jh1nfe43m9****",
  "OverlayMode": "Ipsec",
  "State": "published",
  "Weight": 100,
  "CreateTime": 1563873294331,
  "NextHop": "vco-bp1tui07ob10fmuro****"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.

HttpCode	Error code	Error message	Description
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.5.7. ModifyVpnPbrRouteEntryWeight

Modifies the weight of a policy-based route of a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyVpnPbrRouteEntryWeight	The operation that you want to perform. Set the value to ModifyVpnPbrRouteEntryWeight .
NewWeight	Integer	Yes	100	The new weight you want to set for the policy-based route. 0: specifies a low priority for the route entry. 100: specifies a high priority for the route entry.  Note If two policy-based route entries are configured with the same destination CIDR block, you cannot set the weights of both route entries to 100.
NextHop	String	Yes	vco-bp15oes1py4i66rmd****	The next hop of the policy-based route.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the policy-based route is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
RouteDest	String	Yes	10.0.0.0/24	The destination CIDR block of the policy-based route.
RouteSource	String	Yes	192.168.1.0/24	The source CIDR block of the policy-based route.
VpnGatewayId	String	Yes	vpn-bp1a3kqjiiq9legfx****	The ID of the VPN gateway.
Weight	Integer	Yes	0	The original weight of the policy-based route. Valid values: 0 and 100 .
ClientToken	String	No	d7d24a21-f4ba-4454-9173-b3828dae492b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
OverlayMode	String	No	Ipsec	The overlay mode. Set the value to Ipsec (IPsec tunneling).

Response parameters

Parameter	Type	Example	Description
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyVpnPbrRouteEntryWeight
&NewWeight=100
&NextHop=vco-bp15oes1py4i66rmd****
&RegionId=cn-qingdao-env66-d01
&RouteDest=10.0.0.0/24
&RouteSource=192.168.1.0/24
&VpnGatewayId=vpn-bp1a3kqjiiq9legfx****
&Weight=0
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyVpnPbrRouteEntryWeightResponse>
  <RequestId>5BE01CD7-5A50-472D-AC14-CA181C5C03BE</RequestId>
</ModifyVpnPbrRouteEntryWeightResponse>
```

JSON **format**

```
{
  "RequestId": "E82612A9-CB90-4D7E-B394-1DB7F6509B29"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidVpnGatewayInstancelId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.5.8. DeleteVpnPbrRouteEntry

Deletes a policy-based route from a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteVpnPbrRouteEntry	The operation that you want to perform. Set the value to DeleteVpnPbrRouteEntry .
NextHop	String	Yes	vco-bp15oes1py4i66rmd****	The next hop of the policy-based route.
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the policy-based route is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
RouteDest	String	Yes	10.0.0.0/24	The destination CIDR block of the policy-based route.
RouteSource	String	Yes	192.168.1.0/24	The source CIDR block of the policy-based route.
VpnGatewayId	String	Yes	vpn-bp1a3kqjiiq9legfx****	The ID of the VPN gateway.
Weight	Integer	Yes	0	The weight of the policy-based route. Valid values: 0: specifies a low priority for the route. 100: specifies a high priority for the route entry. Note If two policy-based route entries are configured with the same destination CIDR block, you cannot set the weights of both route entries to 100.

Parameter	Type	Required	Example	Description
ClientToken	String	No	d7d24a21-f4ba-4454-9173-b3828dae492b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
OverlayMode	String	No	Ipsec	The overlay mode. Set the value to Ipsec (IPsec tunneling).

Response parameters

Parameter	Type	Example	Description
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteVpnPbrRouteEntry
&NextHop=vco-bp15oes1py4i66rmd****
&RegionId=cn-qingdao-env66-d01
&RouteDest=10.0.0.0/24
&RouteSource=192.168.1.0/24
&VpnGatewayId=vpn-bp1a3kqjiq9legfx****
&Weight=0
<Common request parameters>
```

Sample success responses

XML format

```
<DeleteVpnPbrRouteEntryResponse>
  <RequestId>5BE01CD7-5A50-472D-AC14-CA181C5C03BE</RequestId>
</DeleteVpnPbrRouteEntryResponse>
```

JSON format

```
{
  "RequestId": "E82612A9-CB90-4D7E-B394-1DB7F6509B29"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.5.9. DescribeVpnPbrRouteEntries

Queries policy-based routes of a VPN gateway.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpnPbrRouteEntries	The operation that you want to perform. Set the value to DescribeVpnPbrRouteEntries .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the policy-based routes are created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnGatewayId	String	Yes	vpn-bp1a3kqjii9legfx****	The ID of the VPN gateway.
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
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.
TotalCount	Integer	12	The number of returned entries.
VpnPbrRouteEntries	Array of VpnPbrRouteEntry		The detailed information about the policy-based routes.
VpnPbrRouteEntry			
CreateTime	Long	1492747187000	The timestamp generated when the policy-based route was created.
NextHop	String	vco-bp15oes1py4i66rmd****	The next hop of the policy-based route.
RouteDest	String	10.0.0.0/24	The destination CIDR block of the policy-based route.
RouteSource	String	192.xx.0.0/24	The source CIDR block of the policy-based route.
State	String	published	The status of the policy-based route. Valid values: published: The route is advertised. normal: The route is not advertised.
VpnInstanceId	String	vpn-bp1cmw7jh1nfe43m9****	The ID of the VPN gateway.
Weight	Integer	0	The weight of the policy-based route. Valid values: 0: indicates that the priority of the route entry is low. 100: indicates that the priority of the route entry is high.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVpnPbrRouteEntries
&RegionId=cn-qingdao-env66-d01
&VpnGatewayId=vpn-bp1a3kqjii9legfx****
&<<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVpnPbrRouteEntriesResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <RequestId>E5D94DC7-AEC7-4E73-A203-61B04D1F1160</RequestId>
  <PageSize>10</PageSize>
  <VpnPbrRouteEntries>
    <VpnPbrRouteEntry>
      <RouteDest>10.0.0.0/32</RouteDest>
      <VpnInstanceId>vpn-bp1cmw7jhlufe43m9****</VpnInstanceId>
      <State>published</State>
      <Weight>100</Weight>
      <CreateTime>1563881012000</CreateTime>
      <NextHop>vco-bp1tui07ob10fmuro****</NextHop>
      <RouteSource>11.0.0.0/32</RouteSource>
    </VpnPbrRouteEntry>
  </VpnPbrRouteEntries>
</DescribeVpnPbrRouteEntriesResponse>
```

JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "RequestId": "E5D94DC7-AEC7-4E73-A203-61B04D1F1160",
  "PageSize": 10,
  "VpnPbrRouteEntries": {
    "VpnPbrRouteEntry": [
      {
        "RouteDest": "10.0.0.0/32",
        "VpnInstanceId": "vpn-bp1cmw7jhlufe43m9****",
        "State": "published",
        "Weight": 100,
        "CreateTime": 1563881012000,
        "NextHop": "vco-bp1tui07ob10fmuro****",
        "RouteSource": "11.0.0.0/32"
      }
    ]
  }
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.

6.6. IPsec-VPN

6.6.1. CreateVpnConnection

Creates an IPsec-VPN connection.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateVpnConnection	The operation that you want to perform. Set the value to CreateVpnConnection .
CustomerGatewayId	String	Yes	vpn-bp1q8bgx4xnk****	The ID of the customer gateway.
LocalSubnet	String	Yes	10.1.1.0/24,10.1.2.0/24	The CIDR block of the virtual private cloud (VPC) that is used to connect with the data center. This CIDR block is used in Phase 2 negotiations. Separate multiple CIDR blocks with commas (.). Example: 192.168.1.0/24,192.168.2.0/24.
RegionId	String	Yes	cn-qingdao-env66-d01	The region ID of the IPsec-VPN connection. You can call the <code>DescribeRegions</code> operation to query the most recent region list.

Parameter	Type	Required	Example	Description
RemoteSubnet	String	Yes	10.10.1.0/24,10.10.2.0/24	The CIDR block of the data center. The peer CIDR block is used in Phase 2 negotiations. Separate multiple CIDR blocks with commas (.). Example: 192.168.3.0/24,192.168.4.0/24.
VpnGatewayId	String	Yes	vpn-bp1q8bgx4xnkm****	The ID of the VPN gateway.
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 a token, but you must make sure that the token is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.
Name	String	No	IPsec	The name of the IPsec-VPN connection. 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 <code>http://</code> or <code>https://</code> .
EffectImmediately	Boolean	No	false	Specifies whether to delete the current IPsec tunnel and reinitiate negotiations. Valid values: true: initiates negotiations after the configuration is completed. false: initiates negotiations when inbound traffic is detected. This is the default value.
IkeConfig	String	No	<pre>{"IkeVersion": "ikev1", "IkeMode": "main", "IkeEncAlg": "aes", "IkeAuthAlg": "sha1", "IkePfs": "group2", "IkeLifetime": 86400}</pre>	The configuration of Phase 1 negotiations: IkeConfig.Psk: the pre-shared key that is used to authenticate the VPN gateway and the customer gateway. By default, a random value is generated. You can also specify a pre-shared key. The description cannot exceed 100 characters in length. IkeConfig.IkeVersion: The version of the IKE protocol. Valid values: ikev1 and ikev2. Default value: ikev1. IkeConfig.IkeMode: the negotiation mode of IKE V1. Valid values: main and aggressive. Default value: main. IkeConfig.IkeEncAlg: The encryption algorithm used in Phase 1 negotiations. Valid values: aes, aes192, aes256, des, and 3des. Default value: aes. IkeConfig.IkeAuthAlg: The authentication algorithm used in Phase 1 negotiations. Valid values: md5 and sha1. Default value: md5. IkeConfig.IkePfs: The Diffie-Hellman key exchange algorithm used in Phase 1 negotiations. Valid values: group1, group2, group5, group14, and group24. Default value: group2. IkeConfig.IkeLifetime: the SA lifetime as a result of Phase 1 negotiations. Valid values: 0 to 86400. Unit: seconds. Default value: 86400. IkeConfig.LocalIdIPsec: the identifier of the VPN gateway. This parameter can contain up to 100 characters. The default value is the public IP address of the VPN gateway. IkeConfig.Remoteld: the identifier of the customer gateway. This parameter can contain up to 100 characters. By default, it is the public IP address of the customer gateway.

Parameter	Type	Required	Example	Description
IpssecConfig	String	No	<code>{"IpssecEncAlg":"aes","IpssecAuthAlg":"sha1","IpssecPfs":"group2","IpssecLifetime":86400}</code>	The configuration of Phase 2 negotiations: IpssecConfig.IpssecEncAlg: The encryption algorithm used in Phase 2 negotiations. Valid values: <code>aes</code>, <code>aes192</code>, <code>aes256</code>, <code>des</code>, and <code>3des</code>. Default value: <code>aes</code>. IpssecConfig.IpssecAuthAlg: The authentication algorithm used in Phase 2 negotiations. Valid values: <code>md5</code> and <code>sha1</code>. Default value: <code>md5</code>. IpssecConfig.IpssecPfs: the Diffie-Hellman group for perfect forward secrecy (PFS). If you set this parameter, the system forwards packets of all protocols. The Diffie-Hellman key exchange algorithm used in Phase 2 negotiations. Valid values: <code>group1</code>, <code>group2</code>, <code>group5</code>, <code>group14</code>, and <code>group24</code>. Default value: <code>group2</code>. IpssecConfig.IpssecLifetime: the SA lifetime as a result of Phase 2 negotiations. Valid values: <code>0</code> to <code>86400</code>. Unit: seconds. Default value: <code>86400</code>.
HealthCheckConfig	String	No	<code>{"enable":"true","dip":"192.168.xx.2","sip":"192.168.xx.2","interval":"3","retry":"3"}</code>	The health check configuration: HealthCheckConfig.enable: specifies whether to enable health checks. Valid values: <code>true</code> and <code>false</code>. Default value: <code>false</code>. HealthCheckConfig.dip: the destination IP address configured for health checks. HealthCheckConfig.sip: the source IP address configured for health checks. HealthCheckConfig.interval: the time interval of health check retries. Unit: seconds. HealthCheckConfig.retry: the maximum number of health check retries.
AutoConfigRoute	Boolean	No	<code>true</code>	Specifies whether to automatically configure routes. Valid values: true: enables automatic configuration. false: disables automatic configuration. This is the default value.

Response parameters

Parameter	Type	Example	Description
VpnConnectionId	String	<code>vco-bp15oes1py4i6****</code>	The ID of the IPsec-VPN connection.
CreateTime	Long	<code>1544666102000</code>	The timestamp generated when the IPsec-VPN connection was created.
Name	String	<code>test</code>	The name of the IPsec-VPN connection.
RequestId	String	<code>082AD562-B8DB-4BB2-861F-DA1FCA01FD76</code>	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateVpnConnection
&CustomerGatewayId=vpn-bp1q8bgx4xnk****
&LocalSubnet=10.1.1.0/24,10.1.2.0/24
&RegionId=cn-qingdao-env66-d01
&RemoteSubnet=10.10.1.0/24,10.10.2.0/24
&VpnGatewayId=vpn-bp1q8bgx4xnk****
&<Common request parameters>
```

Sample success responses

XML format

```
<CreateVpnConnectionResponse>
  <VpnConnectionId>vco-bp1bbi27hojx8****</VpnConnectionId>
  <CreateTime>1493363928000</CreateTime>
</CreateVpnConnectionResponse>
```

JSON format

```
{
  "CreateTime": 1544666102000,
  "VpnConnectionId": "vco-bp15oes1py4i6****"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
404	InvalidCustomerGatewayInstancelId.NotFound	The specified customer gateway instance id does not exist.	The error message returned because the specified instance ID does not exist.
404	InvalidVpnGatewayInstancelId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	InvalidVpnConnection.AlreadyExists	Vpn connection already exists.	The error message returned because the IPsec-VPN connection already exists.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.6.2. ModifyVpnConnectionAttribute

Modifies the configuration of an IPsec-VPN connection.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyVpnConnectionAttribute	The operation that you want to perform. Set the value to ModifyVpnConnectionAttribute .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the IPsec-VPN connection is created. You can call the DescribeRegions operation to query the most recent region list.
VpnConnectionId	String	Yes	vco-bp1bbi27hojx80nck****	The ID of the IPsec-VPN connection.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token is used to ensure the idempotence of the request. You can use the client to generate a token, but you must make sure that the token is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.
Name	String	No	IPsec	The name of the IPsec-VPN connection. The name must be 2 to 128 characters in length, and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter. However, the name cannot start with <code>http://</code> or <code>https://</code> .
LocalSubnet	String	No	10.1.1.0/24,10.1.2.0/24	The CIDR block of the virtual private cloud (VPC) that is used to connect with the data center. This CIDR block is used in Phase 2 negotiations. Separate multiple CIDR blocks with commas (,). Example: 192.168.1.0/24,192.168.2.0/24.
RemoteSubnet	String	No	10.10.1.0/24,10.10.2.0/24	The CIDR block of the data center. This CIDR block is used in Phase 2 negotiations. Separate multiple CIDR blocks with commas (,). Example: 192.168.3.0/24,192.168.4.0/24.

Parameter	Type	Required	Example	Description
EffectImmediately	Boolean	No	false	Specifies whether to delete the current IPsec tunnel and reinitiate negotiations. Valid values: true: initiates negotiations after the configuration is completed. false: initiates negotiations when inbound traffic is detected. This is the default value.
IkeConfig	String	No	<pre>{"IkeVersion": "ikev1", "IkeMode": "main", "IkeEncAlg": "aes", "IkeAuthAlg": "sha1", "IkePfs": "group2", "IkeLifetime": 86400}</pre>	The configuration of Phase 1 negotiations: IkeConfig.Psk: the pre-shared key that is used to authenticate the VPN gateway and the customer gateway. You can specify a key or use the default key that is randomly generated by the system. The key must be 1 to 100 characters in length. IkeConfig.IkeVersion: the version of the IKE protocol. Valid values: ikev1 and ikev2. Default value: ikev1. IkeConfig.IkeMode: the negotiation mode of IKE V1. Valid values: main and aggressive. Default value: main. IkeConfig.IkeEncAlg: The encryption algorithm of Phase 1 negotiations. Valid values: aes, aes192, aes256, des, and 3des. Default value: aes. IkeConfig.IkeAuthAlg: The authentication algorithm of Phase 1 negotiations. Valid values: md5 and sha1. Default value: sha1. IkeConfig.IkePfs: The Diffie-Hellman key exchange algorithm of Phase 1 negotiations. Valid values: group1, group2, group5, group14, and group24. Default value: group2. IkeConfig.IkeLifetime: the SA lifetime as a result of Phase 1 negotiations. Valid values: 0 to 86400. Unit: seconds. Default value: 86400. IkeConfig.LocalIdIPsec: the identifier of the VPN gateway. This parameter can contain up to 100 characters. By default, it is the public IP address of the VPN gateway. IkeConfig.Remoteld: the identifier of the customer gateway. This parameter can contain up to 100 characters. By default, it is the public IP address of the customer gateway.
IpsecConfig	String	No	<pre>{"IpsecEncAlg": "aes", "IpsecAuthAlg": "sha1", "IpsecPfs": "group2", "IpsecLifetime": 86400}</pre>	The configuration of Phase 2 negotiations: IpsecConfig.IpsecEncAlg: The encryption algorithm of Phase 2 negotiations. Valid values: aes, aes192, aes256, des, and 3des. Default value: aes. IpsecConfig.IpsecAuthAlg: The authentication algorithm of Phase 2 negotiations. Valid values: md5 and sha1. Default value: sha1. IpsecConfig.IpsecPfs: the Diffie-Hellman group for perfect forward secrecy (PFS). If you set this parameter, the system forwards packets of all protocols. The Diffie-Hellman key exchange algorithm of Phase 2 negotiations. Valid values: group1, group2, group5, group14, and group24. Default value: group2. IpsecConfig.IpsecLifetime: the SA lifetime as a result of Phase 2 negotiations. Valid values: 0 to 86400. Unit: seconds. Default value: 86400.
HealthCheckConfig	String	No	<pre>{"enable": "true", "dip": "192.168.xx.2", "sip": "192.168.xx.2", "interval": "3", "retry": "3"}</pre>	The health check configuration: HealthCheckConfig.enable: specifies whether to enable health checks. Valid values: true and false. Default value: false. HealthCheckConfig.dip: the destination IP address configured for the health check. HealthCheckConfig.sip: the source IP address configured for the health check. HealthCheckConfig.interval: the time interval of health check retries. Unit: seconds. HealthCheckConfig.retry: the maximum number of health check retries.
AutoConfigRoute	Boolean	No	true	Specifies whether to automatically advertise routes. Valid values: true: enables automatic advertising. false: disables automatic advertising. This is the default value.

Response parameters

Parameter	Type	Example	Description
-----------	------	---------	-------------

Parameter	Type	Example	Description
VpnConnectionId	String	vco-bp1bbi27hojx80nck****	The ID of the IPsec-VPN connection.
CustomerGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the customer gateway.
VpnGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.
Name	String	test	The name of the IPsec-VPN connection.
LocalSubnet	String	10.1.1.0/24,10.1.2.0/24	The CIDR block of the VPC.
RemoteSubnet	String	10.10.1.0/24,10.10.2.0/24	The CIDR block of the data center.
CreateTime	Long	1492753817000	The timestamp generated when the IPsec-VPN connection was created.
Description	String	description	The description of the IPsec-VPN connection.
EffectImmediately	Boolean	false	Indicates whether IPsec-VPN negotiations are initiated immediately. Valid values: true: initiates negotiations after the configuration is completed. false: initiates negotiations when inbound traffic is detected.
IkeConfig	Struct		The configuration of Phase 1 negotiations.
IkeAuthAlg	String	sha1	The IKE authentication algorithm.
IkeEncAlg	String	aes	The IKE encryption algorithm.
IkeLifetime	Long	86400	The IKE lifetime.
IkeMode	String	main	The IKE mode.
IkePfs	String	group2	The DH group.
IkeVersion	String	ikev1	The IKE version.
LocalId	String	116.XX.XX.64	The local ID. The default value is the IP address of the VPN gateway. Both fully qualified domain names (FQDNs) and IP addresses are supported.
Psk	String	pgw6dy7d1i8i****	The pre-shared key.
RemoteId	String	139.XX.XX.167	The peer ID. The default value is the IP address of the customer gateway. Both FQDNs and IP addresses are supported.
IpsecConfig	Struct		The configuration of Phase 2 negotiations.
IpsecAuthAlg	String	sha1	The IPsec authentication algorithm.
IpsecEncAlg	String	aes	The IPsec encryption algorithm.
IpsecLifetime	Long	86400	The IPsec lifetime.
IpsecPfs	String	group2	The DH group.
RequestId	String	7DB79D0C-5F27-4AB5-995B-79BE55102F90	The ID of the request.
VcoHealthCheck	Struct		The health check configuration.
Dip	String	1.XX.XX.1	The destination IP address.

Parameter	Type	Example	Description
Enable	String	true	Indicates whether health checks are enabled. Valid values: true: Health checks are enabled. false: Health checks are disabled.
Interval	Integer	3	The interval between two consecutive health checks. Unit: seconds.
Retry	Integer	1	The maximum number of health check retries.
Sip	String	2.XX.XX.2	The source IP address.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyVpnConnectionAttribute
&RegionId=cn-qingdao-env66-d01
&VpnConnectionId=vco-bp1bbi27hojx80nck****
&<Common request parameters>
```

Sample success responses

XML **format**

```
<ModifyVpnConnectionAttributeResponse>
  <Name>vpn</Name>
  <CustomerGatewayId>cgw-bp1pvpl9r9adju615****</CustomerGatewayId>
  <RemoteSubnet>172.16.2.0/24</RemoteSubnet>
  <IpsecConfig>
    <IpsecLifetime>86400</IpsecLifetime>
    <IpsecAuthAlg>sha1</IpsecAuthAlg>
    <IpsecPfs>group2</IpsecPfs>
    <IpsecEncAlg>aes</IpsecEncAlg>
  </IpsecConfig>
  <EffectImmediately>>false</EffectImmediately>
  <VpnGatewayId>vpn-bp1q8bgx4xnkm2ogj****</VpnGatewayId>
  <CreateTime>1492753817000</CreateTime>
  <VpnConnectionId>vco-bp10lz7aejumd2vxo****</VpnConnectionId>
  <RequestId>57070A3D-38F2-40A6-A1C9-DB14542EF54D</RequestId>
  <LocalSubnet>10.1.1.0/24,10.1.2.0/24</LocalSubnet>
  <IkeConfig>
    <IkeEncAlg>aes</IkeEncAlg>
    <RemoteId>139.XX.XX.32</RemoteId>
    <IkePfs>group2</IkePfs>
    <IkeAuthAlg>sha1</IkeAuthAlg>
    <Psk>pgw6dy7dli8i****</Psk>
    <IkeMode>main</IkeMode>
    <IkeLifetime>86400</IkeLifetime>
    <IkeVersion>ikev1</IkeVersion>
    <LocalId>116.XX.XX.69</LocalId>
  </IkeConfig>
</ModifyVpnConnectionAttributeResponse>
```

JSON **format**

```
{
  "Name": "vpn",
  "CustomerGatewayId": "cgw-bp1pvpl9r9adju615****",
  "RemoteSubnet": "172.16.2.0/24",
  "IpsecConfig": {
    "IpsecLifetime": 86400,
    "IpsecAuthAlg": "sha1",
    "IpsecPfs": "group2",
    "IpsecEncAlg": "aes"
  },
  "EffectImmediately": false,
  "VpnGatewayId": "vpn-bp1q8bgx4xnkm2ogj****",
  "CreateTime": 1492753817000,
  "VpnConnectionId": "vco-bp101z7aejumd2vxo****",
  "RequestId": "7DB79D0C-5F27-4AB5-995B-79BE55102F90",
  "LocalSubnet": "10.1.1.0/24,10.1.2.0/24",
  "IkeConfig": {
    "IkeEncAlg": "aes",
    "RemoteId": "139.XX.XX.32",
    "IkePfs": "group2",
    "IkeAuthAlg": "sha1",
    "Psk": "pgw6dy7d1i8i****",
    "IkeMode": "main",
    "IkeLifetime": 86400,
    "IkeVersion": "ikev1",
    "LocalId": "116.XX.XX.69"
  }
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidVpnConnectionInstanceId.NotFound	The specified vpn connection instance id does not exist.	The error message returned because the specified IPsec-VPN connection does not exist. You can check whether the configuration of the connection is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.
400	InvalidName	The name is not valid	The error message returned because the specified name is in an invalid format.

6.6.3. DescribeVpnConnections

Queries one or more IPsec-VPN connections.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpnConnections	The operation that you want to perform. Set the value to DescribeVpnConnections .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the IPsec-VPN connections are created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnGatewayId	String	No	vpn-bp1q8bgx4xnkx****	The ID of the VPN gateway.
CustomerGatewayId	String	No	cgw-bp1mvj4g9kogw****	The ID of the customer gateway.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.

Parameter	Type	Required	Example	Description
PageSize	Integer	No	10	The number of entries to return on each page. Maximum value: 50 . Default value: 10 .
VpnConnectionId	String	No	vco-bp15oes1py4i6****	The ID of the IPsec-VPN connection.

Response parameters

Parameter	Type	Example	Description
VpnConnections	Array of VpnConnection		The detailed information about the IPsec-VPN connections.
VpnConnection			
IkeConfig	Struct		The configuration of Phase 1 negotiations.
IkeAuthAlg	String	sha1	The IKE authentication algorithm. Valid values: sha1 and MD5 .
IkeEncAlg	String	aes	The IKE encryption algorithm.
IkeLifetime	Long	86400	The IKE lifetime. Unit: seconds.
IkeMode	String	main	The IKE mode. Valid values: main and aggressive . The main mode offers higher security. If NAT traversal is enabled, we recommend that you select the aggressive mode.
IkePfs	String	group2	The DH group. Valid values: group1 , group2 , group5 , group14 , and group24 .
IkeVersion	String	ikev1	The IKE version.
LocalId	String	116.XX.XX.64	The local ID. The default value is the IP address of the VPN gateway. Both fully qualified domain names (FQDNs) and IP addresses are supported.
Psk	String	pgw6dy7d****	The pre-shared key.
RemotId	String	139.XX.XX.167	The peer ID. The default value is the IP address of the customer gateway. Both FQDNs and IP addresses are supported.
IpsecConfig	Struct		The configuration of Phase 2 negotiations.
IpsecAuthAlg	String	sha1	The IPsec authentication algorithm. Valid values: sha1 and md5 .
IpsecEncAlg	String	aes	The IPsec encryption algorithm.
IpsecLifetime	Long	86400	The IPsec lifetime.
IpsecPfs	String	group2	The DH group.
VpnConnectionId	String	vco-bp10lz7aejumd****	The ID of the IPsec-VPN connection.
CustomerGatewayId	String	cgw-bp1mvj4g9kogw****	The ID of the customer gateway.
VpnGatewayId	String	vpn-bp1q8bgx4xnkm****	The ID of the VPN gateway.
Name	String	name	The name of the IPsec-VPN connection.
LocalSubnet	String	10.1.1.0/24,10.1.2.0/24	The CIDR block of the VPC.
RemoteSubnet	String	10.10.1.0/24,10.10.2.0/24	The CIDR block of the data center.

Parameter	Type	Example	Description
CreateTime	Long	1492753817000	The timestamp generated when the IPsec-VPN connection was created.
Status	String	ipsec_sa_established	The status of the IPsec-VPN connection. Valid values: ike_sa_not_established: indicates that Phase 1 negotiations failed. ike_sa_established: indicates that Phase 1 negotiations succeeded. ipsec_sa_not_established: indicates that Phase 2 negotiations failed. ipsec_sa_established: indicates that Phase 2 negotiations succeeded.
EffectImmediately	Boolean	true	Indicates whether IPsec-VPN negotiations are initiated immediately. Valid values: true: Negotiations are reinitiated when the configuration is changed. false: Negotiations are reinitiated when traffic is detected. When negotiations are reinitiated, transient connections may occur.
VcoHealthCheck	Struct		The configuration of health checks.
Dip	String	8.XX.XX.8	The destination IP address.
Enable	String	true	Indicates whether health checks are enabled. Valid values: true: Health checks are enabled. false: Health checks are disabled.
Interval	Integer	2	The interval between two consecutive health checks. Unit: seconds.
Retry	Integer	1	The maximum number of health check retries.
Sip	String	192.XX.XX.66	The source IP address that is used for health checks.
Status	String	failed	The status of the health check. Valid values: failed: The health check failed. success: The health check was successful.
TotalCount	Integer	10	The number of entries.
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned on each page.
RequestId	String	54A4B3D0-DF4D-4C54-B8DC-5DC8DD49C939	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVpnConnections
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML [format](#)

```
<DescribeVpnConnections>
  <PageNumber>1</PageNumber>
  <VpnConnections>
    <VpnConnection>
      <Name>VPN connection test</Name>
      <CustomerGatewayId>cgw-bp1pvpl9r9adjxxxxxxxx</CustomerGatewayId>
      <RemoteSubnet>172.16.2.0/24</RemoteSubnet>
      <IpsecConfig>
        <IpsecLifetime>86400</IpsecLifetime>
        <IpsecAuthAlg>sha1</IpsecAuthAlg>
        <IpsecPfs>group2</IpsecPfs>
        <IpsecEncAlg>aes</IpsecEncAlg>
      </IpsecConfig>
      <EffectImmediately>true</EffectImmediately>
      <VpnGatewayId>vpn-bp1q8bgx4xnkmxxxxxxxx</VpnGatewayId>
      <CreateTime>1492753817000</CreateTime>
      <VpnConnectionId>vco-bp101z7aejumdxxxxxxxx</VpnConnectionId>
      <status>ipsec_sa_established</status>
      <LocalSubnet>10.1.1.0/24,10.1.2.0/24</LocalSubnet>
      <IkeConfig>
        <IkeEncAlg>aes</IkeEncAlg>
        <RemoteId>139.XX.XX.167</RemoteId>
        <IkePfs>group2</IkePfs>
        <IkeAuthAlg>sha1</IkeAuthAlg>
        <Psk>pgw6dy****</Psk>
        <IkeMode>main</IkeMode>
        <IkeLifetime>86400</IkeLifetime>
        <IkeVersion>ikev1</IkeVersion>
        <LocalId>116.XX.XX.64</LocalId>
      </IkeConfig>
    </VpnConnection>
  </VpnConnections>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>54A4B3D0-DF4D-4C54-B8DC-5DC8DD49C939</RequestId>
</DescribeVpnConnections>
```

JSON format

```
{
  "PageNumber": 1,
  "VpnConnections": {
    "VpnConnection": [
      {
        "Name": "vpn connection test",
        "CustomerGatewayId": "cgw-bp1pvpl9r9adjxxxxxxxx",
        "RemoteSubnet": "172.16.2.0/24",
        "IpsecConfig": {
          "IpsecLifetime": 86400,
          "IpsecAuthAlg": "sha1",
          "IpsecPfs": "group2",
          "IpsecEncAlg": "aes"
        },
        "EffectImmediately": true,
        "VpnGatewayId": "vpn-bp1q8bgx4xnkmxxxxxxxx",
        "CreateTime": 1492753817000,
        "VpnConnectionId": "vco-bp101z7aejumdxxxxxxxx",
        "status": "ipsec_sa_established",
        "LocalSubnet": "10.1.1.0/24,10.1.2.0/24",
        "IkeConfig": {
          "IkeEncAlg": "aes",
          "RemoteId": "139.XX.XX.167",
          "IkePfs": "group2",
          "IkeAuthAlg": "sha1",
          "Psk": "pgw6dy****",
          "IkeMode": "main",
          "IkeLifetime": 86400,
          "IkeVersion": "ikev1",
          "LocalId": "116.XX.XX.64"
        }
      }
    ]
  },
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "54A4B3D0-DF4D-4C54-B8DC-5DC8DD49C939"
}
```

Error codes

HttpCode	Error code	Error message	Description
----------	------------	---------------	-------------

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.

6.6.4. DescribeVpnConnection

Queries the details of an IPsec-VPN connection.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpnConnection	The operation that you want to perform. Set the value to DescribeVpnConnection .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the IPsec-VPN connection is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnConnectionId	String	Yes	vco-bp1bbi27hojx80nck****	The ID of the IPsec-VPN connection.

Response parameters

Parameter	Type	Example	Description
VpnConnectionId	String	vco-bp1bbi27hojx80nck****	The ID of the IPsec-VPN connection.
CustomerGatewayId	String	cgw-bp1mvj4g9kogwwcxk****	The ID of the customer gateway.
VpnGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.
Name	String	ipsec1	The name of the IPsec-VPN connection.
LocalSubnet	String	10.1.1.0/24,10.1.2.0/24	The CIDR block of the VPC.
RemoteSubnet	String	10.10.1.0/24,10.10.2.0/24	The CIDR block of the data center.
CreateTime	Long	1492753817000	The time when the IPsec-VPN connection was created.
Status	String	ike_sa_not_established	The status of the IPsec-VPN connection. Valid values: ike_sa_not_established: indicates that Phase 1 negotiations failed. ike_sa_established: indicates that Phase 1 negotiations succeeded. ipsec_sa_not_established: indicates that Phase 2 negotiations failed. ipsec_sa_established: indicates that Phase 2 negotiations succeeded.
EffectImmediately	Boolean	true	Indicates whether the IPsec-VPN connection immediately takes effect. Valid values: true: Negotiations are reinitiated when the configuration is changed. false: Negotiations are reinitiated when traffic is detected. When negotiations are reinitiated, transient connections may occur.
IkeConfig	Struct		The configuration of Phase 1 negotiations.
IkeAuthAlg	String	sha1	The IKE authentication algorithm.
IkeEncAlg	String	aes	The IKE encryption algorithm.
IkeLifetime	Long	86400	The IKE lifetime.

Parameter	Type	Example	Description
IkeMode	String	main	The IKE mode. Both main and aggressive modes are supported. The main mode provides higher security. If NAT traversal is enabled, we recommend that you select the aggressive mode.
IkePfs	String	group2	The DH group.
IkeVersion	String	ikev1	The IKE version.
LocalId	String	116.XX.XX.69	The local ID. The default value is the IP address of the VPN gateway. Both fully qualified domain names (FQDNs) and IP addresses are supported.
Psk	String	pgw6dy7d18in7x5	The pre-shared key.
Remoteld	String	139.XX.XX.32	The peer ID. The default value is the IP address of the customer gateway. Both FQDNs and IP addresses are supported.
IpssecConfig	Struct		The configuration of Phase 2 negotiations.
IpssecAuthAlg	String	sha1	The IPsec authentication algorithm.
IpssecEncAlg	String	aes	The IPsec encryption algorithm.
IpssecLifetime	Long	86400	The IPsec lifetime.
IpssecPfs	String	group2	The DH group.
RequestId	String	F2310D45-BCF6-4E2E-9082-B4503844BA4C	The ID of the request.
VcoHealthCheck	Struct		The information about health checks.
Dip	String	10.XX.XX.1	The destination IP address.
Enable	String	true	Indicates whether health checks are enabled. Valid values: false: Health checks are disabled. true: Health checks are enabled.
Interval	Integer	3	The interval between two consecutive health checks. Unit: seconds.
Retry	Integer	3	The maximum number of health check retries.
Sip	String	192.XX.XX.2	The source IP address for health checks.
Status	String	failed	The status of the health check.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVpnConnection
&RegionId=cn-qingdao-env66-d01
&VpnConnectionId=vco-bp1bbi27hojx80nck***
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVpnConnectionResponse>
  <PageNumber>1</PageNumber>
  <VpnConnections>
    <VpnConnection>
      <Name>c2</Name>
      <CustomerGatewayId>cgw-bp1w18dtz3auwlvw****</CustomerGatewayId>
      <Status>ike_sa_not_established</Status>
      <RemoteSubnet>192.168.0.0/16</RemoteSubnet>
      <IpsecConfig>
        <IpsecLifetime>86400</IpsecLifetime>
        <IpsecAuthAlg>md5</IpsecAuthAlg>
        <IpsecPfs>group2</IpsecPfs>
        <IpsecEncAlg>aes</IpsecEncAlg>
      </IpsecConfig>
      <EffectImmediately>>false</EffectImmediately>
      <VpnGatewayId>vpn-bplyfrjxn4d5t63tb****</VpnGatewayId>
      <CreateTime>1519391420000</CreateTime>
      <VpnConnectionId>vco-bp1w3mlp23iftycv****</VpnConnectionId>
      <LocalSubnet>172.16.0.0/12</LocalSubnet>
      <IkeConfig>
        <IkeEncAlg>aes</IkeEncAlg>
        <RemoteId>47.XX.XX.176</RemoteId>
        <IkePfs>group2</IkePfs>
        <IkeAuthAlg>sha1</IkeAuthAlg>
        <Psk>1234567</Psk>
        <IkeMode>aggressive</IkeMode>
        <IkeLifetime>86400</IkeLifetime>
        <IkeVersion>ikev1</IkeVersion>
        <LocalId>116.XX.XX.119</LocalId>
      </IkeConfig>
    </VpnConnection>
  </VpnConnections>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>7D598A10-26EF-44F2-9F47-E417842F3CEA</RequestId>
</DescribeVpnConnectionResponse>
```

JSON format

```
{
  "PageNumber": 1,
  "VpnConnections": {
    "VpnConnection": [
      {
        "Name": "c2",
        "CustomerGatewayId": "cgw-bp1w18dtz3auwlvw****",
        "Status": "ike_sa_not_established",
        "RemoteSubnet": "192.168.0.0/16",
        "IpsecConfig": {
          "IpsecLifetime": 86400,
          "IpsecAuthAlg": "md5",
          "IpsecPfs": "group2",
          "IpsecEncAlg": "aes"
        },
        "EffectImmediately": false,
        "VpnGatewayId": "vpn-bplyfrjxn4d5t63tb****",
        "CreateTime": 1519391420000,
        "VpnConnectionId": "vco-bp1w3mlp23iftycv****",
        "LocalSubnet": "172.16.0.0/12",
        "IkeConfig": {
          "IkeEncAlg": "aes",
          "RemoteId": "47.XX.XX.176",
          "IkePfs": "group2",
          "IkeAuthAlg": "sha1",
          "Psk": "1234567",
          "IkeMode": "aggressive",
          "IkeLifetime": 86400,
          "IkeVersion": "ikev1",
          "LocalId": "116.XX.XX.119"
        }
      }
    ]
  },
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "7D598A10-26EF-44F2-9F47-E417842F3CEA"
}
```

Error codes

HttpCode	Error code	Error message	Description
----------	------------	---------------	-------------

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidVpnConnectionInstanceId.NotFound	The specified vpn connection instance id does not exist.	The error message returned because the specified IPsec-VPN connection does not exist. Check whether the ID of the IPsec-VPN connection is valid.

6.6.5. DownloadVpnConnectionConfig

Queries the configuration of an IPsec-VPN connection.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DownloadVpnConnectionConfig	The operation that you want to perform. Set the value to DownloadVpnConnectionConfig .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the IPsec-VPN connection is created. You can call the DescribeRegions operation to query the most recent region list.
VpnConnectionId	String	Yes	vco-bp1bbi27hojx80nck****	The ID of the IPsec-VPN connection.

Response parameters

Parameter	Type	Example	Description
RequestId	String	0C68048B-0F70-40DA-B8AE-1B79B5CF62E3	The ID of the request.
VpnConnectionConfig	Struct		The configuration of the IPsec-VPN connection.
IkeConfig	Struct		The IKE configuration.
IkeAuthAlg	String	sha1	The IKE authentication algorithm. Valid values: sha1 and md5 .
IkeEncAlg	String	aes	The IKE encryption algorithm.
IkeLifetime	Long	86400	The IKE lifetime. Unit: seconds.
IkeMode	String	main	The IKE mode. Valid values: main and aggressive . The main mode offers higher security. If NAT traversal is enabled, we recommend that you select the aggressive mode.
IkePfs	String	group2	The DH group.
IkeVersion	String	ikev1	The IKE version.
LocalId	String	116.XX.XX.69	The local ID. The default value is the IP address of the VPN gateway. Both fully qualified domain names (FQDNs) and IP addresses are supported.
Psk	String	pgw6dy7d18i****	The pre-shared key.
RemoteId	String	139.XX.XX.32	The peer ID. The default value is the IP address of the customer gateway. Both FQDNs and IP addresses are supported.
IpssecConfig	Struct		The configuration of the IPsec-VPN connection.
IpssecAuthAlg	String	sha1	The IPsec authentication algorithm. Valid values: sha1 and md5 .

Parameter	Type	Example	Description
IpsecEncAlg	String	aes	The IPsec encryption algorithm.
IpsecLifetime	Long	86400	The IPsec lifetime. Unit: seconds.
IpsecPfs	String	group2	The DH group.
Local	String	139.XX.XX.32	The ID of the VPN gateway.
LocalSubnet	String	10.1.1.0/24,10.1.2.0/24	The CIDR block of the VPC.
Remote	String	116.XX.XX.69	The ID of the customer gateway.
RemoteSubnet	String	10.10.1.0/24,10.10.2.0/24	The CIDR block of the data center.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DownloadVpnConnectionConfig
&RegionId=cn-qingdao-env66-d01
&VpnConnectionId=vco-bplbbi27hojx80nck****
&<Common request parameters>
```

Sample success responses

XML format

```
<DownloadVpnConnectionConfigResponse>
  <RequestId>0C68048B-0F70-40DA-B8AE-1B79B5CF62E3</RequestId>
  <VpnConnectionConfig>
    <RemoteSubnet>10.10.1.0/24,10.10.2.0/24</RemoteSubnet>
    <Local>139.XX.XX.32</Local>
    <IpsecConfig>
      <IpsecLifetime>86400</IpsecLifetime>
      <IpsecAuthAlg>sha1</IpsecAuthAlg>
      <IpsecPfs>group2</IpsecPfs>
      <IpsecEncAlg>aes</IpsecEncAlg>
    </IpsecConfig>
    <Remote>116.XX.XX.69x</Remote>
    <LocalSubnet>172.16.2.0/24</LocalSubnet>
    <IkeConfig>
      <IkeEncAlg>aes</IkeEncAlg>
      <IkePfs>group2</IkePfs>
      <RemoteId>116.XX.XX.69</RemoteId>
      <IkeAuthAlg>sha1</IkeAuthAlg>
      <Psk>pgw6dy7dli8i****</Psk>
      <IkeMode>main</IkeMode>
      <IkeLifetime>86400</IkeLifetime>
      <IkeVersion>ikev1</IkeVersion>
      <LocalId>139.XX.XX.32</LocalId>
    </IkeConfig>
  </VpnConnectionConfig>
</DownloadVpnConnectionConfigResponse>
```

JSON format

```
{
  "RequestId": "0C68048B-0F70-40DA-B8AE-1B79B5CF62E3",
  "VpnConnectionConfig": {
    "RemoteSubnet": "10.10.1.0/24,10.10.2.0/24",
    "Local": "139.XX.XX.32",
    "IpsecConfig": {
      "IpsecLifetime": 86400,
      "IpsecAuthAlg": "sha1",
      "IpsecPfs": "group2",
      "IpsecEncAlg": "aes"
    },
    "Remote": "116.XX.XX.69",
    "LocalSubnet": "172.16.2.0/24",
    "IkeConfig": {
      "IkeEncAlg": "aes",
      "IkePfs": "group2",
      "RemoteId": "116.XX.XX.69",
      "IkeAuthAlg": "sha1",
      "Psk": "pgw6dy7d1i8i****",
      "IkeMode": "main",
      "IkeLifetime": 86400,
      "IkeVersion": "ikev1",
      "LocalId": "139.XX.XX.32"
    }
  }
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform the operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidVpnConnectionInstanceId.NotFound	The specified vpn connection instance id does not exist.	The error message returned because the specified IPsec-VPN connection does not exist. Check whether the ID of the IPsec-VPN connection is valid.

6.6.6. DeleteVpnConnection

Deletes a specified IPsec-VPN connection.

Note After an IPsec-VPN connection between a virtual private cloud (VPC) and a data center is deleted, the communication between the VPC and data center is interrupted.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteVpnConnection	The operation that you want to perform. Set the value to DeleteVpnConnection .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the IPsec-VPN connection is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnConnectionId	String	Yes	vco-bp1bbi27hojx80nck****	The ID of the IPsec-VPN connection.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token is used to ensure the idempotence of the request. You can use the client to generate a token, but you must make sure that the token 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
-----------	------	---------	-------------

Parameter	Type	Example	Description
RequestId	String	606998F0-B94D-48FE-8316-ACA81BB230DA	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteVpnConnection
&RegionId=cn-qingdao-env66-d01
&VpnConnectionId=vco-bp1bbi27hojx80nck****
&<Common request parameters>
```

Sample success responses

XML format

```
<DeleteVpnConnectionResponse>
  <RequestId>606998F0-B94D-48FE-8316-ACA81BB230DA</RequestId>
</DeleteVpnConnectionResponse>
```

JSON format

```
{
  "RequestId": "606998F0-B94D-48FE-8316-ACA81BB230DA"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
404	InvalidVpnConnectionInstanceId.NotFound	The specified vpn connection instance id does not exist.	The error message returned because the specified IPsec-VPN connection does not exist. Check whether the ID of the IPsec-VPN connection is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.

6.7. SSL-VPN

6.7.1. CreateSslVpnServer

Creates an SSL-VPN server.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateSslVpnServer	The operation that you want to perform. Set the value to CreateSslVpnServer .
ClientIpPool	String	Yes	192.168.1.0/24	The CIDR block that is allocated to the virtual network interface of the client. It is not the CIDR block where the client resides. When the client accesses the server through an SSL-VPN connection, the VPN gateway selects an IP address from the specified CIDR block and assigns it to the client. This CIDR block must not conflict with the value of LocalSubnet .
LocalSubnet	String	Yes	10.0.0.0/8	The CIDR block to be accessed by the client through the SSL-VPN connection. You can set the value to the CIDR block of a VPC, a vSwitch, a data center that is connected to the VPC through an Express Connect circuit, or an Alibaba Cloud service, such as ApsaraDB RDS or OSS.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the VPN gateway is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnGatewayId	String	Yes	vpn-bp1hgim8by0kc9nga****	The ID of the VPN gateway.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
Name	String	No	sslvpnname	The name of the SSL-VPN server. The name must be 2 to 128 characters in length and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter, but cannot start with <code>http://</code> or <code>https://</code> .
Proto	String	No	UDP	The protocol that is used by the SSL-VPN server. Valid values: TCP: TCP. UDP: UDP. This is the default value.
Cipher	String	No	AES-128-CBC	The encryption algorithm that is used in the SSL-VPN connection. Valid values: AES-128-CBC: the AES-128-CBC algorithm. This is the default value. AES-192-CBC: the AES-192-CBC algorithm. AES-256-CBC: the AES-256-CBC algorithm. none: If the parameter is set to this value, no encryption algorithm is used.
Port	Integer	No	1194	The port that is used by the SSL-VPN server. Default value: 1194 . The following ports cannot be used: 22, 2222, 22222, 9000, 9001, 9002, 7505, 80, 443, 53, 68, 123, 4510, 4560, 500, and 4500.
Compress	Boolean	No	false	Specifies whether to enable data compression. Valid values: true: enables data compression. false: disables data compression. This is the default value.

Response parameters

Parameter	Type	Example	Description
Name	String	test	The name of the SSL-VPN server.
RequestId	String	E98A9651-7098-40C7-8F85-C818D1EBBA85	The ID of the request.
SslVpnServerId	String	vss-bp18q7hzj6largv4v****	The ID of the SSL-VPN server.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateSslVpnServer
&ClientIpPool=192.168.1.0/24
&LocalSubnet=10.0.0.0/8
&RegionId=cn-qingdao-env66-d01
&VpnGatewayId=vpn-bp1hgim8by0kc9nga****
<Common request parameters>
```

Sample success responses

`XML` `format`

```
<CreateSslVpnServerResponse>
  <RequestId>E98A9651-7098-40C7-8F85-C818D1EBBA85</RequestId>
  <SslVpnServerId>vss-bp18q7hzj6largv4v****</SslVpnServerId>
  <Name>test</Name>
</CreateSslVpnServerResponse>
```

JSON format

```
{
  "RequestId": "E98A9651-7098-40C7-8F85-C818D1EBBA85",
  "SslVpnServerId": "vss-bp18q7hzj6largv4v****",
  "Name": "test"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
400	InvalidName	The name is not valid	The error message returned because the format of the specified name is invalid.
404	InvalidVpnGatewayInstanceId.NotFound	The specified vpn gateway instance id does not exist.	The error message returned because the specified VPN gateway does not exist. Check whether the configuration of the VPN gateway is valid.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.7.2. ModifySslVpnServer

Modifies the configuration of an SSL-VPN server.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifySslVpnServer	The operation that you want to perform. Set the value to ModifySslVpnServer .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the VPN gateway is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
SslVpnServerId	String	Yes	vss-bp18q7hzj6largv4v****	The ID of the SSL-VPN server.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
Name	String	No	test	The name of the SSL-VPN server. 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 <code>http://</code> or <code>https://</code> .
ClientIpPool	String	No	10.30.30.0/24	The client IP address pool.

Parameter	Type	Required	Example	Description
LocalSubnet	String	No	10.20.20.0/24	The CIDR block of the VPC.
Proto	String	No	UDP	The protocol that is used by the SSL-VPN server. Valid values: TCP: TCP UDP: UDP. This is the default value.
Cipher	String	No	AES-128-CBC	The encryption algorithm that is used in the SSL-VPN connection. Valid values: AES-128-CBC: the AES-128-CBC algorithm. This is the default value. AES-192-CBC: the AES-192-CBC algorithm. AES-256-CBC: the AES-256-CBC algorithm. none: If the parameter is set to this value, no encryption algorithm is used.
Port	Integer	No	1194	The port that is used by the SSL-VPN server. Default value: 1194 . The following ports cannot be used: 22, 2222, 22222, 9000, 9001, 9002, 7505, 80, 443, 53, 68, 123, 4510, 4560, 500, and 4500 .
Compress	Boolean	No	false	Specifies whether to enable data compression. Valid values: true: enables data compression. false: disables data compression. This is the default value.

Response parameters

Parameter	Type	Example	Description
Cipher	String	AES-128-CBC	The encryption algorithm.
ClientIpPool	String	10.30.30.0/24	The client IP address pool.
Compress	Boolean	false	Indicates whether data compression is enabled.
Connections	Integer	0	The total number of current connections.
CreateTime	Long	1492753580000	The time when the SSL-VPN server was created.
InternetIp	String	47.XX.XX.98	The public IP address.
LocalSubnet	String	10.20.20.0/24	The CIDR block of the VPC.
MaxConnections	Integer	5	The maximum number of connections.
Name	String	test	The name of the SSL-VPN server.
Port	Integer	1194	The port that is used by the SSL-VPN server.
Proto	String	UDP	The protocol that is used by the SSL-VPN server.
RegionId	String	cn-qingdao-env66-d01	The region ID of the SSL-VPN server.
RequestId	String	DF11D6F6-E35A-41C3-9B20-6FC8A901FE65	The ID of the request.
SslVpnServerId	String	vss-bp18q7hzj6largv4v****	The ID of the SSL-VPN server.
VpnGatewayId	String	vpn-bp1q8bgx4xnkm2ogj****	The ID of the VPN gateway.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifySslVpnServer
&RegionId=cn-qingdao-env66-d01
&SslVpnServerId=vss-bp18q7hzj6largv4v****
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifySslVpnServerResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <SslVpnServers>
    <SslVpnServer>
      <RegionId>cn-qingdao-env66-d01</RegionId>
      <SslVpnServerId>vss-bp18q7hzj6largv4v****</SslVpnServerId>
      <VpnGatewayId>vpn-bp1q8bgx4xnkm2ogj****</VpnGatewayId>
      <Name>test</Name>
      <ClientIpPool>10.30.30.0/24</ClientIpPool>
      <LocalSubnet>10.20.20.0/24</LocalSubnet>
      <Proto>UDP</Proto>
      <Port>1194</Port>
      <Cipher>AES-128-CBC</Cipher>
      <Compress>true</Compress>
      <CreateTime>1492753580000</CreateTime>
      <Connections>0</Connections>
      <MaxConnections>5</MaxConnections>
      <InternetIp>47.XX.XX.98</InternetIp>
    </SslVpnServer>
  </SslVpnServers>
  <RequestId>DF11D6F6-E35A-41C3-9B20-6FC8A901FE65</RequestId>
</ModifySslVpnServerResponse>
```

JSON format

```
{
  "PageNumber": "1",
  "TotalCount": "1",
  "PageSize": "10",
  "SslVpnServers": {
    "SslVpnServer": {
      "RegionId": "cn-qingdao-env66-d01",
      "SslVpnServerId": "vss-bp18q7hzj6largv4v****",
      "VpnGatewayId": "vpn-bp1q8bgx4xnkm2ogj****",
      "Name": "test",
      "ClientIpPool": "10.30.30.0/24",
      "LocalSubnet": "10.20.20.0/24",
      "Proto": "UDP",
      "Port": "1194",
      "Cipher": "AES-128-CBC",
      "Compress": "true",
      "CreateTime": "1492753580000",
      "Connections": "0",
      "MaxConnections": "5",
      "InternetIp": "47.XX.XX.98"
    }
  },
  "RequestId": "DF11D6F6-E35A-41C3-9B20-6FC8A901FE65"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	InvalidName	The name is not valid	The error message returned because the specified name is in an invalid format.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.7.3. DescribeSslVpnServers

Queries one or more SSL-VPN servers.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSslVpnServers	The operation that you want to perform. Set the value to DescribeSslVpnServers .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN servers are created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
SslVpnServerId	String	No	vss-bp15j3du13gq1dgey****	The ID of the SSL-VPN server.
VpnGatewayId	String	No	vpn-bp1on0xae9d771ggi****	The ID of the VPN gateway.
Name	String	No	test	The name of the SSL-VPN server.
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
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned on each page.
RequestId	String	085CA5EA-1E76-43A8-981B-E0208DECA0CB	The ID of the request.
SslVpnServers	Array of SslVpnServer		The detailed information about the SSL-VPN servers.
SslVpnServer			
Cipher	String	AES-128-CBC	The encryption algorithm.
ClientIpPool	String	10.10.1.0/24	The client IP address pool.
Compress	Boolean	false	Indicates whether the transmitted data is compressed.
Connections	Integer	0	The total number of current connections.
CreateTime	Long	1544668844000	The timestamp generated when the SSL-VPN server was created.
InternetIp	String	47.XX.XX.167	The public IP address.
LocalSubnet	String	192.168.0.0/24	The CIDR block of the client.
MaxConnections	Integer	5	The maximum number of connections.
Name	String	test	The name of the SSL-VPN server.
Port	Integer	1194	The port that is used by the SSL-VPN server.
Proto	String	UDP	The protocol that is used by the SSL-VPN server.
RegionId	String	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN server is created.

Parameter	Type	Example	Description
SslVpnServerId	String	vss-bp15j3du13gq1dgey****	The ID of the SSL-VPN server.
VpnGatewayId	String	vpn-bp1on0xae9d771ggi****	The ID of the VPN gateway.
TotalCount	Integer	1	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSslVpnServers
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeSslVpnServersResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <SslVpnServers>
    <SslVpnServer>
      <RegionId>cn-qingdao-env66-d01</RegionId>
      <SslVpnServerId>vss-bp18q7hzj6largv4v****</SslVpnServerId>
      <VpnGatewayId>vpn-bp1q8bgx4xnkm2ogj****</VpnGatewayId>
      <Name>test</Name>
      <ClientIpPool>10.10.10.0/24</ClientIpPool>
      <LocalSubnet>10.10.20.0/24</LocalSubnet>
      <Proto>UDP</Proto>
      <Port>1194</Port>
      <Cipher>AES-128-CBC</Cipher>
      <Compress>true</Compress>
      <CreateTime>1492753580000</CreateTime>
      <Connections>0</Connections>
      <MaxConnections>5</MaxConnections>
      <InternetIp>47.XX.XX.167</InternetIp>
    </SslVpnServer>
  </SslVpnServers>
  <RequestId>DF11D6F6-E35A-41C3-9B20-6FC8A901FE65</RequestId>
</DescribeSslVpnServersResponse>
```

JSON format

```
{
  "PageNumber": "1",
  "TotalCount": "1",
  "PageSize": "10",
  "SslVpnServers": {
    "SslVpnServer": {
      "RegionId": "cn-qingdao-env66-d01",
      "SslVpnServerId": "vss-bp18q7hzj6largv4v****",
      "VpnGatewayId": "vpn-bp1q8bgx4xnkm2ogj****",
      "Name": "test",
      "ClientIpPool": "10.10.10.0/24",
      "LocalSubnet": "10.10.20.0/24",
      "Proto": "UDP",
      "Port": "1194",
      "Cipher": "AES-128-CBC",
      "Compress": "true",
      "CreateTime": "1492753580000",
      "Connections": "0",
      "MaxConnections": "5",
      "InternetIp": "47.XX.XX.167"
    }
  },
  "RequestId": "DF11D6F6-E35A-41C3-9B20-6FC8A901FE65"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.

HttpCode	Error code	Error message	Description
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.

6.7.4. DescribeVpnSslServerLogs

Queries the logs of an SSL-VPN server.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpnSslServerLogs	The operation that you want to perform. Set the value to DescribeVpnSslServerLogs .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN server is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
VpnSslServerId	String	Yes	vss-bp155e9yclsg1xgq4****	The name of the SSL-VPN server.
From	Integer	No	2018020201	The beginning of the time range to query. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. If the From parameter is set, you must set the To or MinutePeriod parameter.
To	Integer	No	2018020206	The end of the time range to query. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. If the From parameter is set, you must set the To or MinutePeriod parameter.
MinutePeriod	Integer	No	10	The cycle of the logs. If the From and To parameters are not set, you must set the MinutePeriod parameter.
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
Count	Integer	10	The number of log entries.
Data	List	test	An array of log entries. Each item in the array indicates a log entry.
IsCompleted	Boolean	true	Indicates whether the log data is accurate. Valid values: true: accurate false: inaccurate
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	1	The number of entries returned per page.
RequestId	String	5BE01CD7-5A50-472D-AC14-CA1B1C5C03BE	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVpnSslServerLogs
&RegionId=cn-qingdao-env66-d01
&VpnSslServerId=vss-bp155e9yclsg1xgq4****
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVpnSslServerLogsResponse>
  <Data></Data>
  <PageNumber>1</PageNumber>
  <Count>0</Count>
  <PageSize>10</PageSize>
  <IsCompleted>true</IsCompleted>
  <RequestId>26641E42-66C7-4942-9FEC-F99213914F8F</RequestId>
</DescribeVpnSslServerLogsResponse>
```

JSON format

```
{
  "Data": {
    "Logs": []
  },
  "PageNumber": 1,
  "Count": 0,
  "PageSize": 10,
  "IsCompleted": true,
  "RequestId": "26641E42-66C7-4942-9FEC-F99213914F8F"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.

6.7.5. DeleteSslVpnServer

Deletes an SSL-VPN server.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteSslVpnServer	The operation that you want to perform. Set the value to DeleteSslVpnServer .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN server is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
SslVpnServerId	String	Yes	vss-bp18q7hzj6largv4v****	The ID of the SSL-VPN server.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	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	606998F0-B94D-48FE-8316-ACA81BB230DA	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteSslVpnServer
&RegionId=cn-qingdao-env66-d01
&SslVpnServerId=vss-bp18q7hzj6largv4v****
&<Common request parameters>
```

Sample success responses

XML format

```
<DeleteSslVpnServerResponse>
  <RequestId>606998F0-B94D-48FE-8316-ACA81BB230DA</RequestId>
</DeleteSslVpnServerResponse>
```

JSON format

```
{
  "RequestId": "606998F0-B94D-48FE-8316-ACA81BB230DA"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.

6.7.6. CreateSslVpnClientCert

Creates an SSL-VPN client certificate.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateSslVpnClientCert	The operation that you want to perform. Set the value to CreateSslVpnClientCert .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the VPN gateway is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
SslVpnServerId	String	Yes	vss-m5et0q3iy1qex328w****	The ID of the SSL-VPN server.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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.
Name	String	No	SslVpnClientCert1	The name of the SSL-VPN client certificate. 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 <code>http://</code> or <code>https://</code> .

Response parameters

Parameter	Type	Example	Description
Name	String	SslVpnClientCert	The name of the SSL-VPN client certificate.
RequestId	String	079874CD-AEC1-43E6-AC03-ADD96B6E4907	The ID of the request.
SslVpnClientCertId	String	vsc-m5euof6s5jy8vs5kd****	The ID of the SSL-VPN client certificate.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateSslVpnClientCert
&RegionId=cn-qingdao-env66-d01
&SslVpnServerId=vss-m5et0q3iylqex328w****
&<Common request parameters>
```

Sample success responses

XML **format**

```
<CreateSslVpnClientCertResponse>
  <SslVpnClientCertId>vsc-bp1n8wcf134yl0osr****</SslVpnClientCertId>
  <RequestId>606998F0-B94D-48FE-8316-ACA81BB230DA</RequestId>
</CreateSslVpnClientCertResponse>
```

JSON **format**

```
{
  "SslVpnClientCertId": "vsc-bp1n8wcf134yl0osr****",
  "RequestId": "606998F0-B94D-48FE-8316-ACA81BB230DA"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	Resource.QuotaFull	The quota of resource is full	The error message returned because the resource quota is reached.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.
400	VpnGateway.FinancialLocked	The specified service is financial locked.	The error message returned because the service is suspended due to overdue payments. Top up your account first.
400	InvalidName	The name is not valid	The error message returned because the specified name is in an invalid format.

6.7.7. ModifySslVpnClientCert

Modifies the name of an SSL-VPN client certificate.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifySslVpnClientCert	The operation that you want to perform. Set the value to ModifySslVpnClientCert .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN client certificate is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
SslVpnClientCertId	String	Yes	vsc-bp1n8wcf134yl0osr****	The ID of the SSL-VPN client certificate.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, but you must make sure that the token is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.

Parameter	Type	Required	Example	Description
Name	String	No	cert2	The name of the SSL-VPN client certificate. The name must be 2 to 128 characters in length and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter. However, the name cannot start with <code>http://</code> or <code>https://</code> .

Response parameters

Parameter	Type	Example	Description
Name	String	cert2	The name of the SSL-VPN client certificate.
RequestId	String	606998F0-B94D-48FE-8316-ACA81BB230DA	The ID of the request.
SslVpnClientCertId	String	vsc-bp1n8wcf134yl0osr****	The ID of the SSL-VPN client certificate.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifySslVpnClientCert
&RegionId=cn-qingdao-env66-d01
&SslVpnClientCertId=vsc-bp1n8wcf134yl0osr****
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifySslVpnClientCertResponse>
  <SslVpnClientCertId>vsc-bp1n8wcf134yl0osr****</SslVpnClientCertId>
  <Name>cert2</Name>
  <RequestId>606998F0-B94D-48FE-8316-ACA81BB230DA</RequestId>
</ModifySslVpnClientCertResponse>
```

JSON format

```
{
  "SslVpnClientCertId": "vsc-bp1n8wcf134yl0osr****",
  "Name": "cert2",
  "RequestId": "606998F0-B94D-48FE-8316-ACA81BB230DA"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	InvalidName	The name is not valid	The error message returned because the specified name is in an invalid format.

6.7.8. DescribeSslVpnClientCerts

Queries one or more SSL-VPN client certificates.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSslVpnClientCerts	The operation that you want to perform. Set the value to DescribeSslVpnClientCerts .
RegionId	String	Yes	cn-qingdao-env66-d01	The region ID of the SSL-VPN client certificates to be queried. You can call the <code>DescribeRegions</code> operation to query the most recent region list.

Parameter	Type	Required	Example	Description
SslVpnServerId	String	No	vss-bp18q7hzj6largv4v****	The ID of the SSL-VPN server.
SslVpnClientCertId	String	No	vsc-bp1n8wcf134yl0osr****	The ID of the SSL-VPN client certificate.
Name	String	No	cert1	The name of the SSL-VPN client certificate.
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
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.
SslVpnClientCertKeys	Array of SslVpnClientCertKey		The detailed information about the queried SSL client certificates.
SslVpnClientCertKey			
CreateTime	Long	1492747187000	The timestamp generated when the SSL client certificate was created.
EndTime	Long	1494966335000	The time to be generated when the SSL client certificate expires.
Name	String	cert1	The name of the SSL-VPN client certificate.
RegionId	String	cn-qingdao-env66-d01	The region ID of the SSL-VPN client certificate.
SslVpnClientCertId	String	vsc-bp1n8wcf134yl0osr****	The ID of the SSL-VPN client certificate.
SslVpnServerId	String	vss-bp18q7hzj6largv4v****	The ID of the SSL-VPN server.
Status	String	normal	The status of the SSL-VPN client certificate. Valid values: expiring-soon: The SSL-VPN client certificate expires in one week. normal: The certificate is normal. expired: The certificate has expired.
TotalCount	Integer	1	The number of returned entries.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSslVpnClientCerts
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

[XML](#) [format](#)

```
<DescribeSslVpnServersResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <SslVpnServers>
    <SslVpnServer>
      <RegionId>cn-qingdao-env66-d01</RegionId>
      <SslVpnServerId>vss-bp18q7hzj6largv4v****</SslVpnServerId>
      <VpnGatewayId>vpn-bp1q8bgx4xnkm2ogj****</VpnGatewayId>
      <Name>test</Name>
      <ClientIpPool>10.10.20.0/24</ClientIpPool>
      <LocalSubnet>10.10.10.0/24</LocalSubnet>
      <Proto>UDP</Proto>
      <Port>1194</Port>
      <Cipher>AES-128-CBC</Cipher>
      <Compress>true</Compress>
      <CreateTime>1492753580000</CreateTime>
      <Connections>0</Connections>
      <MaxConnections>5</MaxConnections>
      <InternetIp>47.XX.XX.98</InternetIp>
    </SslVpnServer>
  </SslVpnServers>
  <RequestId>DF11D6F6-E35A-41C3-9B20-6FC8A901FE65</RequestId>
</DescribeSslVpnServersResponse>
```

JSON format

```
{
  "DescribeSslVpnServersResponse": {
    "PageNumber": "1",
    "TotalCount": "1",
    "PageSize": "10",
    "SslVpnServers": {
      "SslVpnServer": {
        "RegionId": "cn-qingdao-env66-d01",
        "SslVpnServerId": "vss-bp18q7hzj6largv4v****",
        "VpnGatewayId": "vpn-bp1q8bgx4xnkm2ogj****",
        "Name": "test",
        "ClientIpPool": "10.10.20.0/24",
        "LocalSubnet": "10.10.10.0/24",
        "Proto": "UDP",
        "Port": "1194",
        "Cipher": "AES-128-CBC",
        "Compress": "true",
        "CreateTime": "1492753580000",
        "Connections": "0",
        "MaxConnections": "5",
        "InternetIp": "47.XX.XX.98"
      }
    },
    "RequestId": "DF11D6F6-E35A-41C3-9B20-6FC8A901FE65"
  }
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.

6.7.9. DescribeSslVpnClientCert

Queries a specified SSL-VPN client certificate.

Request parameters

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

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN client certificate that you want to query is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
SslVpnClientCertId	String	Yes	vsc-bp17r58rjf5r1gjyr****	The ID of the SSL-VPN client certificate that you want to query.

Response parameters

Parameter	Type	Example	Description
CaCert	String	The CA certificate	The CA certificate.
ClientCert	String	The SSL-VPN client certificate	The SSL-VPN client certificate.
ClientConfig	String	The configuration of the client	The configuration of the client.
ClientKey	String	The key of the client	The key of the client.
CreateTime	Long	1552550980000	The timestamp generated when the SSL-VPN client certificate was created.
EndTime	Long	1647158980000	The timestamp to be generated when the SSL-VPN client certificate expires.
Name	String	abc	The name of the SSL-VPN client certificate.
RegionId	String	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN client certificate is created.
RequestId	String	5BE01CD7-5A50-472D-AC14-CA181C5C03BE	The ID of the request.
SslVpnClientCertId	String	vsc-bp13k5mp4tg8v3z9b****	The ID of the SSL-VPN client certificate.
SslVpnServerId	String	vss-bp155e9yclsg1xgq4****	The ID of the SSL-VPN server.
Status	String	normal	The status of the SSL-VPN client certificate. Valid values: expiring-soon: The SSL-VPN client certificate expires in one week. normal: The certificate is normal. expired: The certificate has expired.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSslVpnClientCert
&RegionId=cn-qingdao-env66-d01
&SslVpnClientCertId=vsc-bp17r58rjf5r1gjyr****
&<Common request parameters>
```

Sample success responses

XML **format**

```
<DescribeSslVpnServersResponse>
  <Name>df</Name>
  <Status>normal</Status>
  <ClientConfig>****</ClientConfig>
  <ClientCert>****</ClientCert>
  <CreateTime>1552550980000</CreateTime>
  <RegionId>cn-qingdao-env66-d01</RegionId>
  <RequestId>49D54005-6E0E-4132-B305-F3A24DEDDC9</RequestId>
  <EndTime>1647158980000</EndTime>
  <SslVpnClientCertId>vsc-bp13k5mp4tg8v3z9b****</SslVpnClientCertId>
  <ClientKey>****</ClientKey>
  <CaCert>****</CaCert>
  <SslVpnServerId>vss-bp155e9yclsg1xgq4****</SslVpnServerId>
</DescribeSslVpnServersResponse>
```

JSON **format**

```
{
  "Name": "df",
  "Status": "normal",
  "ClientConfig": "*****",
  "ClientCert": "*****",
  "CreateTime": 1552550980000,
  "RegionId": "cn-qingdao-env66-d01",
  "RequestId": "49D54005-6E0E-4132-B305-F3A24DEDDDC9",
  "EndTime": 1647158980000,
  "SslVpnClientCertId": "vsc-bp13k5mp4tg8v3z9b****",
  "ClientKey": "*****",
  "CaCert": "*****",
  "SslVpnServerId": "vss-bp155e9yclsglxgq4****"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.

6.7.10. DeleteSslVpnClientCert

Deletes an SSL-VPN client certificate.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteSslVpnClientCert	The operation that you want to perform. Set the value to DeleteSslVpnClientCert .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region where the SSL-VPN client certificate is created. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
SslVpnClientCertId	String	Yes	vsc-bp1n8wcf134yl0osr****	The ID of the SSL-VPN client certificate.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-0016e04115b	The client token that is used to ensure the idempotence of the request. You can use the client to generate a token, 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	606998F0-B94D-48FE-8316-ACA81BB230DA	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DeleteSslVpnClientCert
&RegionId=cn-qingdao-env66-d01
&SslVpnClientCertId=vsc-bp1n8wcf134yl0osr****
&<Common request parameters>
```

Sample success responses

XML format

```
<DeleteSslVpnClientCertResponse>
  <RequestId>606998F0-B94D-48FE-8316-ACA81BB230DA</RequestId>
</DeleteSslVpnClientCertResponse>
```

JSON format

```
{
  "RequestId": "606998F0-B94D-48FE-8316-ACA81BB230DA"
}
```

Error codes

HttpCode	Error code	Error message	Description
403	Forbidden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	The error message returned because you are unauthorized to perform this operation on the specified resource. You can apply for the required permissions and try again.
403	Forbidden	User not authorized to operate on the specified resource.	The error message returned because you are unauthorized to perform the operation on the specified resource. To acquire the required permissions, submit a ticket.
400	VpnGateway.Configuring	The specified service is configuring.	The error message returned because the operation is not allowed when the specified service is being configured. Try again later.

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 directory.

    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

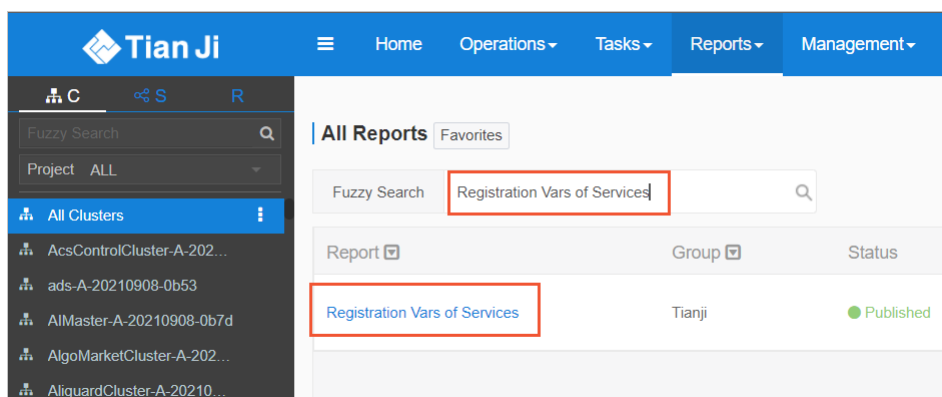
7.2.1. Obtain the endpoint of ASAPI

This topic describes three methods that you can use to obtain an endpoint of Apsara Stack API (ASAPI). This topic also describes how to verify the endpoint.

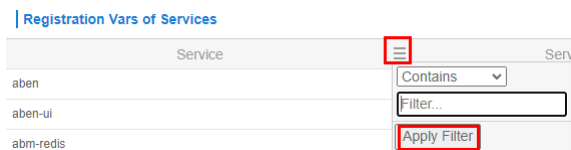
Methods

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

- Log on to the Apsara Infrastructure Management Console.
 - Log on to the Apsara Uni-manager Operations Console.
 - In the top navigation bar, click **Products**.
 - Choose **Platforms > Apsara Infrastructure Management Framework**.
- In the left-side navigation pane, click **Reports**.
- On the **All Reports** page, search for **Registration Vars of Services**. In the report list that appears, click the name of the report.



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



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

- Log on to the Apsara Infrastructure Management Console.
- Go to the cluster operations page.
 - In the left-side navigation pane, choose **Operations > Cluster Operations**.
 - In the **Cluster** search box, enter `ascm`.
 - In the **Actions** column, click **Operations**.
- Obtain the domain value.
 - Click the **Cluster Resources** tab.
 - In the **Name** field, search for `asapi_dns_public`.
 - In the **Application Parameter** column, click **Details**.
In the **Application Parameter** message, obtain the value of the **domain** parameter.

```
{
  "domain": "public.asapi.<region>.cn-****-****-d01.inter.****.****.com",
  "ha_apply_type": "active-active",
  "name": "asapi_dns_public",
  "vip": "10.10.10.10"
}
```

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

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

Method 3: Concatenate strings to generate an endpoint

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

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

Note

- Replace `<region>` with your actual region ID.
- Replace `<internet-domain>` with the root domain of your Apsara Stack service. To obtain the root domain, contact Apsara Stack O&M engineers. Make sure that you use the `internet-domain` parameter instead of the `intranet-domain` parameter.

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

the following endpoint is used as a reference:

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

Verify the 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 these variables with the actual values that you obtained.

Available endpoint example:

```
root@ ~ # curl https://public.asapi.region-id.internet-domain.intranet-domain.asap.asap.com/api/version -k
{"version": "v3.13", "code": "200", "apiCount": 12379, "desc": "update xml pretty"}root@ ~ #
```

Unavailable endpoint example:

```
[root@ ~ # curl https://public.asapi.region-id.internet-domain.intranet-domain.asap.asap.com/api/version -k -i
curl: (35) Peer reports it experienced an internal error.
```

Historical endpoint

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

```
http://server.asapi.region-id.internet-domain.intranet-domain.asapi/v3
```

Note

`region-id` and `intranet-domain` are variables. You must replace these variables with the actual values that you obtained.

Procedure

To obtain the actual values of the `region-id`, `internet-domain`, and `intranet-domain` variables, perform the following steps:

1. In the address bar, enter `region-id.asap.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 current page.

2. Enter your username and password.

Note

Obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

The first time that you log on to the Apsara Uni-manager Operations Console, change the password of your username as prompted.

To enhance security, your password must meet 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 must be 10 to 20 characters in length.

3. Click **Log On** to log on to the **Apsara Uni-manager Operations Console**.
4. In the top navigation bar, choose **Products > Platforms > Apsara Infrastructure Management Framework** to go to the Apsara Infrastructure Management page.
5. In the left-side navigation pane, choose **Operations > Cluster Operations**.
6. On the **Cluster Operations** page, enter `ascm-A` in the Cluster field and click the search icon. Click the cluster name in the **Cluster** column.
7. Click the **Cluster Configuration** tab.
8. On the **File Info** tab of **Cluster Configuration**, click `kv.conf`.
9. In the right window of the displayed page, press Ctrl+F to search for the values of the region, internet-domain, and intranet-domain parameters.

Replace `region-id` with the obtained region value, `internet-domain` with the obtained internet-domain value, and

`intranet-domain` with the obtained intranet-domain value.

Note

Do not include `region-id` in the endpoint of ASAPI that you want to 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

groupId	artifactId	version
com.alibaba	alicrypto-java-aliyun	1.0.4
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?

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

Use a RAM user to obtain an STS token

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 can use the STS token to access Apsara Stack resources.

Benefits

- STS tokens help 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 the validity period for STS tokens. After STS tokens expire, they become invalid. Therefore, you do not need to rotate the 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.
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	wyLT5msyPGP1ohvw8xYgB29dIGi8KMiH2pK****	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.aliyuncs.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 preceding 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.aliyuncs.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	InternalServerError	STS Server Internal Error happened.	The error message returned because an internal server error occurred.