

Alibaba Cloud

Apsara Stack Enterprise

Elastic IP Address Developer Guide

Product Version: v3.16.2

Document Version: 20220830

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	07
1.1. Usage notes on development documentation	07
1.2. Call an API operation	07
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	10
2.4. Obtain an STS AccessKey 3-tuple	12
2.5. Obtain the values of common header parameters	15
2.6. Obtain the endpoint of EIP	17
2.7. Obtain EIP SDK	18
3. Call examples for SDK for Java	20
3.1. Quick start	20
3.2. Use SDK	22
3.2.1. Install SDK for Java	22
3.2.2. Configure authentication credentials	23
3.2.3. Configure connection requests	23
3.2.4. Initiate a request	24
3.2.5. Troubleshooting	25
3.2.6. Use CommonRequest to call API operations	26
4. Call examples for SDK for Python	29
4.1. Quick start	29
4.2. Use SDK	30
4.2.1. Install SDK for Python	30
4.2.2. Configure authentication credentials	31
4.2.3. Set HTTPS requests	31

4.2.4. Initiate a request	32
4.2.5. Handle errors	32
4.2.6. Use CommonRequest to call API operations	33
5.Call examples for SDK for Go	36
5.1. Getting started	36
5.2. Use SDK	37
5.2.1. Install the core package of SDK for Go	37
5.2.2. Configure authentication credentials	37
5.2.3. Initiate a request	38
5.2.4. Handle errors	39
5.2.5. Use CommonRequest to call API operations	40
6.API reference	43
6.1. List of operations by function	43
6.2. Make API requests	43
6.2.1. Request syntax	43
6.2.2. API authorization	44
6.2.3. Signature method guidelines	44
6.3. RAM authentication	45
6.4. Common parameters	47
6.5. Elastic IP addresses	48
6.5.1. AllocateEipAddress	48
6.5.2. AllocateEipAddressPro	54
6.5.3. AssociateEipAddress	59
6.5.4. AllocateEipSegmentAddress	63
6.5.5. DescribeEipSegment	67
6.5.6. ReleaseEipSegmentAddress	70
6.5.7. ModifyEipAddressAttribute	73
6.5.8. DescribeEipAddresses	75

6.5.9. UnassociateEipAddress	86
6.5.10. ReleaseEipAddress	89
6.5.11. DescribeEipGatewayInfo	91
6.5.12. DescribeEipMonitorData	93
6.5.13. MoveResourceGroup	97
6.5.14. DescribeHighDefinitionMonitorLogAttribute	99
7. Appendixes	102
7.1. Process of API calls by using the ASAPI gateway	102
7.2. Use the ASAPI gateway to make API calls	104
7.2.1. Obtain an endpoint of ASAPI	105
7.2.2. Obtain the ASAPI SDK	108
7.3. STS overview	110
7.3.1. What is STS?	110
7.3.2. AssumeRole	110

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 provides the same experience as the public cloud, API operations in Apsara Stack are called by using the POP gateway by default starting Apsara Stack Enterprise V3.16.0. This topic describes how to call API operations in Apsara Stack by using the POP gateway.

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 [Obtain ASAPI SDK](#).

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 an STS AccessKey 3-tuple](#).

Note

We recommend that you use an AccessKey pair or an STS AccessKey 3-tuple 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 ID, 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 [Use developer guides](#).

5. Obtain the endpoint of the cloud service.

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

2. Preparations

2.1. Log on to the API Tool console

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

Prerequisites

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

Procedure

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

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

 **Note** When you log on to the Apsara Uni-manager Management Console for the first time, you must change the password of your account. For security purposes, your password must meet the minimum complexity requirements. The password must be 10 to 32 characters in length and must contain at least two of the following character types:

- Uppercase or lowercase letters
- Digits
- Special characters, which include ! @ # \$ %

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

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

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

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

2.2. Obtain API information

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

Context

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

Procedure

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

2.3. Obtain an AccessKey pair

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

Context

An AccessKey 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 assigned by RAM or STS:

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

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



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

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

Obtain the AccessKey pair of a personal account

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

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

AccessKey Create AccessKey Pair				
The AccessKey ID and AccessKey Secret are the keys used to access the cloud service resources. They have full permissions on the account. Please keep them properly.				
AccessKey ID	AccessKey Secret	Status	Created At	Actions
W1YRFvKH*****	*****	Enable	Sep 18, 2021, 11:05:57	Disable Delete
IsJsAUyX*****	*****	Enable	Sep 10, 2021, 12:28:35	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

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

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

6. In the dialog box that appears, view the AccessKey pair of the organization.

2.4. Obtain an STS AccessKey 3-tuple

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

Background information

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

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

Procedure

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

In the **View Policies of Current Role** dialog box, view your `RAM role`.

2. Obtain the STS AccessKey 3-tuple.

Note

In the following code, replace the 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 STS AccessKey 3-tuple.
    String stsAK = credentials.getString("AccessKeyId");
    String stsSK = credentials.getString("AccessKeySecret");
    String stsToken = credentials.getString("SecurityToken");
}

private static String callAssumeRole(IAcsClient client) {
    CommonRequest request = new CommonRequest();
    // Replace "<sts.aliyuns.com>" with the STS endpoint in the 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 `DescribeEipAddresses` operation of Elastic IP Address (EIP).

 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>", "<yourStsAcces
    skey>", "<yourStsAccessSecret>");
    HttpClientConfig clientConfig = HttpClientConfig.getDefault();
    clientConfig.setIgnoreSSLCerts(true);
    clientConfig.setProtocolType(ProtocolType.HTTPS);
    profile.setHttpClientConfig(clientConfig);
    IAcsClient client = new DefaultAcsClient(profile);
    CommonRequest request = new CommonRequest();
    request.setSysDomain("vpc.aliyuns.com");
    request.setSysProduct("Vpc");
    request.setSysAction("DescribeEipAddresses");
    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
<code>x-acs-regionid</code>	The ID of the region. For more information about how to obtain region IDs, see Obtain a region ID .
<code>x-acs-organizationid</code>	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 .
<code>x-acs-resourcegroupid</code>	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 .
<code>x-acs-instanceid</code>	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 an elastic IP address (EIP), perform the following steps:

1. Log on to the Apsara Uni-manager Management Console.
2. In the top navigation bar, choose **Products > Networking > Elastic IP Address**.

3. In the left-side navigation pane, click **Elastic IP Addresses**.
4. View the IDs and names of EIPs in the **Elastic IP Addresses** list.

Response parameters

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

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

2.6. Obtain the endpoint of EIP

This topic describes how to obtain the endpoint of Elastic IP address (EIP).

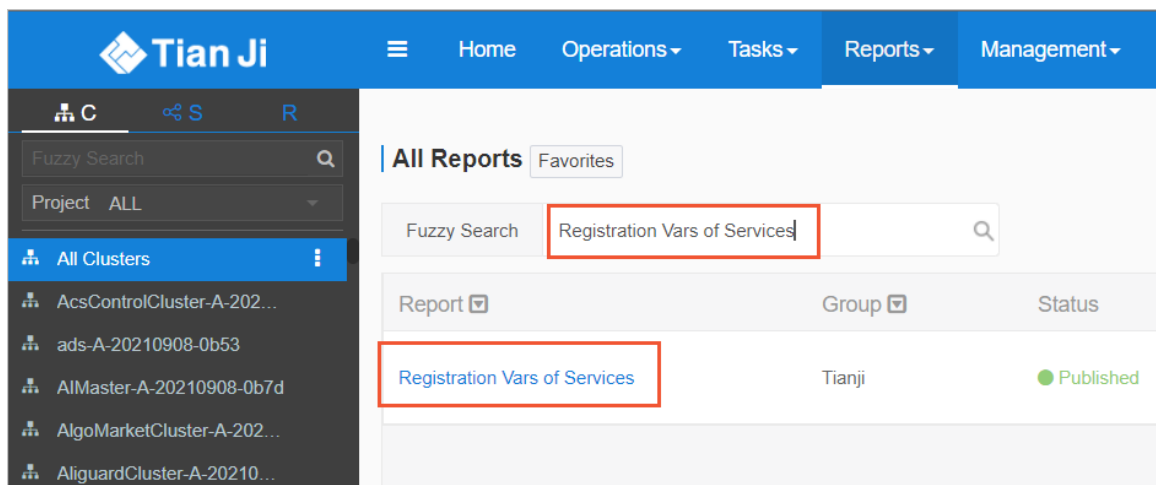
Background information

To use the point of presence (POP) gateway to call API operations in Apsara Stack, you must obtain the service endpoint. You can obtain service endpoints from Apsara Stack onsite O&M engineers. You can also perform the following steps 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, choose **Products > Platforms > Apsara Infrastructure Management Framework**.
2. 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.



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

Note

EIP uses the API service of Virtual Private Cloud (VPC).

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

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

2.7. Obtain EIP SDK

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

Background information

To use the features of Elastic IP address (EIP), you must install Virtual Private Cloud (VPC) SDK and the Alibaba Cloud core library. For example, to use VPC SDK for Java, you must download

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

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

Instructions

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

Note

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

3. Call examples for SDK for Java

3.1. Quick start

This topic describes how to obtain and use Virtual Private Cloud (VPC) SDK for Java. The features of Elastic IP Address (EIP) are implemented by using VPC SDK.

Environment preparation

- You must have an Apsara Stack tenant account and an AccessKey pair (AccessKey ID and AccessKey secret) to use SDK for Java. For more information, see [Obtain an AccessKey pair](#).
- The endpoint of EIP is obtained. For more information, see [Obtain the endpoint of EIP](#).
- To install Alibaba Cloud SDK for Java, you must use Java Development Kit (JDK) 1.8 or later.

Install Alibaba Cloud SDK for Java

If you use Apache Maven to manage a Java project, import the JAR file to the pom.xml file of the project.

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

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

Use Alibaba Cloud SDK for Java

Perform the following steps to use Alibaba Cloud SDK for Java:

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

 Note

Replace the variable parameters in the following sample code with the actual information. Remove the angle brackets (<>) in the final code.

The following section describes the variable parameters:

- Replace <yourRegionID> with the region ID.
- Replace <yourAccessKeyID> with your AccessKey ID.
- Replace <yourAccessKeySecret> with your AccessKey secret.
- Replace <Product> with the service name.
- Replace <Endpoint> with the endpoint of the service.
- Replace <readTimeout> with the read timeout period. Unit: milliseconds.
- Replace <connectionTimeout> with the connection timeout period. Unit: milliseconds.
- Replace <maxRequestsPerHost> with the maximum number of requests for each host.
- Replace <maxRequests> with the maximum number of requests.
- Replace <http://192.168.XX.XX:33XX> with the proxy IP address and port.

```
import com.aliyuncs.http.HttpClientConfig;
import com.aliyuncs.http.ProtocolType;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.vpc.model.v20160428.*;
import com.google.gson.Gson;
public class Main {
    public static void main(String[] args) {
        // Create a DefaultAcsClient instance and initialize the instance.
        DefaultProfile profile = DefaultProfile.getProfile(
            "<yourRegionID>",          // Replace the parameter with the region ID.
            "<yourAccessKeyID>",      // Replace the parameter with your AccessKey ID.
            "<yourAccessKeySecret>"); // Replace the parameter with your AccessKey secret.

        // Replace the parameter with the endpoint of the service.
        profile.addEndpoint("<yourRegionID>", "<Product>", "<Endpoint>");
        // Set the request configuration.
        HttpClientConfig clientConfig = HttpClientConfig.getDefault();
        clientConfig.setIgnoreSSLCerts(true); // Ignore the certificate.
        clientConfig.setReadTimeoutMillis(<readTimeout>); // Optional. Set the read timeout period. Unit: milliseconds.
        clientConfig.setConnectionTimeoutMillis(<connectionTimeout>); // Optional. Set the connection timeout period. Unit: milliseconds.
        clientConfig.setMaxRequestsPerHost(<maxRequestsPerHost>); // Optional. Set the maximum number of requests for each host.
        clientConfig.setMaxRequests(<maxRequests>); // Optional. Set the maximum number of requests.
        clientConfig.setProtocolType(ProtocolType.HTTP); // Optional. Set the request p
```

```
rotocol. Default value: HTTP.
/* Optional. Set the proxy IP address and port.
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 parameters.
DescribeEipAddressesRequest request = new DescribeEipAddressesRequest();
// Service-related parameters.
request.setPageSize(10);
request.setPageNumber(1);
// Set the organization ID and resource set ID for special header parameters. Resources are isolated.
request.putHeaderParameter("x-acs-organizationid", "1");
request.putHeaderParameter("x-acs-resourcegroupid", "11");
// Send the request and handle the response or exception.
DescribeEipAddressesResponse response;
try {
    DescribeEipAddressesResponse 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 SDK for Java

This topic describes how to install and use Virtual Private Cloud (VPC) SDK for Java. The features of Elastic IP Address (EIP) are implemented by using VPC SDK.

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

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

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

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

3.2.2. Configure authentication credentials

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

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

If you want to use your AccessKey pair to access Alibaba Cloud, you must configure the AccessKey pair as a credential when you initialize the client.

Note

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

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

Note

In the preceding sample code, replace the variable parameters with the actual information. Remove the angle 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. The features of Elastic IP Address (EIP) are implemented by using VPC SDK.

Procedure

1. Create an AcsClient instance.

```
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.

```
DescribeEipAddressesRequest request = new DescribeEipAddressesRequest();
// Service-related parameters.
request.setPageSize(10);
request.setPageNumber(1);
// Set the organization ID and resource set ID for special header parameters. Resources
are isolated.
request.putHeaderParameter("x-acs-organizationid", "1");
request.putHeaderParameter("x-acs-resourcegroupid", "");
```

3. Initiate the request and handle the response.

```
DescribeEipAddressesResponse response;
try {
    DescribeEipAddressesResponse 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.e.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 an SDK, or you cannot use an SDK to call API operations whose requests and responses meet your business requirements, you can use CommonRequest to call API operations. You can use CommonRequest to call all API operations.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

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

Use CommonRequest to call an API operation

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

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

You can get the API version from the common parameters in the API documents.

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

You must obtain the Action parameter and specify the API operation by using `request.setSysAction("<Action>")`.

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

Example: Call an RPC API operation

The following code provides an example on how to obtain the information about elastic IP addresses (EIPs) by calling the DescribeEipAddresses operation of EIP. The API of EIP uses RPC.

 **Note** Replace the variable parameters in the following sample code with the actual information. Remove the angle brackets (<>) in the final code.

The following section describes the variable parameters:

- Replace <yourRegionID> with the region ID.
- Replace <yourAccessKeyID> with your AccessKey ID.
- Replace <yourAccessKeySecret> with your AccessKey secret.
- Replace <yourSecurityToken> with your security token.
- Replace <yourResourceGroupID> with the resource set ID.
- Replace <yourOrganizationID> with the organization ID.
- Replace <yourInstanceId> with the instance ID.
- Replace <http://192.168.XX.XX:33XX> with the proxy IP address and port.

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

public class Sample {
    public static void main(String[] args) {
        // Create a DefaultAcsClient instance and initialize the instance.
        DefaultProfile profile = DefaultProfile.getProfile(
            "<yourRegionUD>", // Replace the parameter with the region ID.
            "<yourAccessKeyID>", // Replace the parameter with your AccessKey ID.
            "<yourAccessKeySecret>"); // Replace the parameter with your AccessKey secret.
        HttpClientConfig clientConfig = HttpClientConfig.getDefault();
        clientConfig.setProtocolType(ProtocolType.HTTP);
        /**
         * Specify whether to configure HTTP proxy based on your requirements.
         * To configure HTTP proxy, perform the following steps:
         * clientConfig.setHttpProxy("<http://192.168.XX.XX:33XX>");
         * Replace the parameter with the proxy IP address and port.
         */
        profile.setHttpClientConfig(clientConfig);
        IAcsClient client = new DefaultAcsClient(profile);
        // Create an API request and set the parameters.
        CommonRequest request = new CommonRequest();
        // Replace the parameter with the service domain name
```

```
// Replace the parameter with the service domain name.
request.setSysDomain("vpc.aliyuncs.com");
request.setSysProduct("Vpc");
request.setSysVersion("2016-04-28");
request.setSysAction("DescribeEipAddresses");
request.putQueryParameter("PageNumber", "1");
request.putQueryParameter("PageSize", "30");
request.putHeadParameter("x-acs-resourcegroupid", "<yourResourceGroupID>");// Optional. Specify the resource set ID.
request.putHeadParameter("x-acs-organizationid", "<yourOrganizationID>");// Required. Specify the organization ID.
request.putHeadParameter("x-acs-regionid", "<yourRegionID>");// Optional. Specify the region ID. This parameter is required if you use Apsara Stack Enterprise V3.15.0 or earlier.

// request.putHeadParameter("x-acs-instanceid", "<yourInstanceID>");// Optional. Specify the instance ID. This parameter is required if you want to modify, delete, or query an instance.
/**
 * When you use STS AccessKey credentials to call an API operation, you must add the SecurityToken field in the request parameters.
 * Use the following method:
 * request.putQueryParameter("SecurityToken", "<yourSecurityToken>");
 * Replace the parameter with the actual token.
 */
try {
    CommonResponse response = client.getCommonResponse(request);
    System.out.println(response.getData());
} catch (ServerException e) {
    // TODO Auto-generated catch block
    e.printStackTrace();
} catch (ClientException e) {
    // TODO Auto-generated catch block
    e.printStackTrace();
}
}
```

4. Call examples for SDK for Python

4.1. Quick start

This topic describes how to obtain and use Virtual Private Cloud (VPC) SDK for Python. The features of Elastic IP Address (EIP) are implemented by using VPC SDK.

Environment preparation

- You must have an Apsara Stack tenant account and an AccessKey pair (AccessKey ID and AccessKey secret) to use VPC SDK for Python. For more information, see [Obtain an AccessKey pair](#).
- The endpoint of EIP is obtained. For more information, see [Obtain the endpoint of EIP](#).

Install VPC SDK for Python

1. Install the SDK core library.

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

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

- If you use Python 3.x, run the following command to install the core library of Alibaba Cloud SDK:

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

2. Install VPC SDK for Python.

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

- If you use Python 2.x, run the following command to install VPC SDK:

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

- If you use Python 3.x, run the following command to install VPC SDK:

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

Use VPC SDK for Python

The following steps describe how to use VPC SDK for Python:

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

 **Note** Replace the variable parameters in the following sample code with the actual information. Remove the angle brackets (<>) in the final code.

The following section describes the variable parameters:

- Replace <yourRegionID> with the region ID.
- Replace <yourAccessKeyID> with your AccessKey ID.
- Replace <yourAccessKeySecret> with your AccessKey secret.
- Replace <vpc.aliyuns.com> with the endpoint of the service.

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

4.2. Use SDK

4.2.1. Install SDK for Python

This topic describes how to install and use Virtual Private Cloud (VPC) SDK for Python. The features of Elastic IP Address (EIP) are implemented by using VPC SDK.

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

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

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

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

- If you use Python 3.x, run the following command to install the core library of Alibaba Cloud SDK:

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

The following example describes how to install VPC SDK.

- If you use Python 2.x, run the following command to install VPC SDK:

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

- If you use Python 3.x, run the following command to install VPC SDK:

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

4.2.2. Configure authentication credentials

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

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

If you want to use your AccessKey pair to access Alibaba Cloud, you must configure the AccessKey pair as a credential when you initialize the client.

 **Notice** Do not disclose any code that may contain 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 Virtual Private Cloud (VPC) SDK for Python to initiate a request. The features of Elastic IP Address (EIP) are implemented by using VPC SDK.

Procedure

1. Import VPC SDK.

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

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 = DescribeEipAddressesRequest.DescribeEipAddressesRequest()
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 sdkcore.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 the requests and responses of API operations that you call by using an SDK do not meet your business requirements, you can use CommonRequest to call API operations. You can use CommonRequest to call all API operations.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

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

Use CommonRequest to call an API operation

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

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

You can obtain the API version from the sections about common parameters in the API references.

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

RPC API operation: You must obtain the value of the Action parameter and specify an API operation in `request.set_action_name('Action')`.

For example, if you want to call the DescribeEipAddresses operation, you must use `request.set_action_name('DescribeEipAddresses')` 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 elastic IP addresses (EIPs) by calling the `DescribeEipAddresses` operation of EIP.

 **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.
- <vpc.aliyuncs.com>: Replace the parameter with the endpoint of the service.

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.request import CommonRequest
# Specify the AccessKey ID, the AccessKey secret, and the region ID.
client = AcsClient('{<yourAccessKeyID>}', '{<yourAccessKeySecret>}', '{<yourRegionID>}')
request = CommonRequest()
request.set_product('Vpc')
request.set_action_name('DescribeEipAddresses')
request.set_version('2016-04-28')
request.set_domain('<vpc.aliyuncs.com>') # Replace the variable parameter with the endpoint
of the service.
# or:
# request = CommonRequest(product='Vpc', action_name='DescribeEipAddresses', version='2016-04-28', domain='vpc.aliyuncs.com')
#####
# Specify the request protocol. Valid values: https and http. Default value: http.
# You can specify HTTPS in the following manner:
# request.set_protocol_type('https')
#####
request.set_accept_format('json')
request.set_method('POST')
request.add_query_param('PageNumber', '1')
request.add_query_param('PageSize', '30')
#####
# When you use STS AccessKey credentials 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. Getting started

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 Elastic IP Address (EIP), you must install 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 EIP is obtained. For more information, see [Obtain the endpoint of EIP](#).

Install the core package of Alibaba Cloud SDK for Go

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

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

Use 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 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.
- <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 se
    )
    if err != nil {
        // Handle exceptions.
        panic(err)
    }
    // Create a request and set the required parameters.
    request := vpc.CreateDescribeEipAddressesRequest()
    // 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.DescribeEipAddresses(request)
    if err != nil {
        // Handle exceptions.
        panic(err)
    }
    fmt.Println(response)
}
```

4. Optional. Switch to HTTP or HTTPS.

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

5.2. Use SDK

5.2.1. Install the core package of SDK for Go

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

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

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

5.2.2. Configure authentication credentials

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

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

```
// 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 variable 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 Elastic IP Address (EIP), you must install VPC SDK.

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

1. Import VPC SDK for Go.

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

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

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

```
vpcClient, err := <vpc>.NewClientWithAccessKey( //Replace the parameter with the name o
f the service.
    "<yourRegionID>", // Replace the parameter with the region ID.
    "<yourAccessKeyID>", // Replace the parameter with your AccessKey ID.

    "<yourAccessKeySecret>") // Replace the parameter with your AccessKey secret.
vpcClient.Domain = "vpc.aliyuns.com" //Specify the endpoint of the service.
```

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

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

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

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

4. Initiate the call.

```
response, err := vpcClient.DescribeEipAddresses(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.DescribeEipAddresses(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 VPC SDK for Go:



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.DescribeEipAddresses(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 response of VPC SDK for Go:

 **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.DescribeEipAddresses(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 the requests and responses of API operations that you call by using an SDK do not 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 provides an example on how to obtain the information of elastic IP addresses (EIPs) by calling the DescribeEipAddresses operation of EIP. The API of EIP uses RPC.

 **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.
- <vpc.aliyuncs.com>: Replace the parameter with the endpoint of the service.
- <yourSecurityToken>: Replace the parameter with your security token.
- <yourResourceGroupID>: Replace the parameter with the resource set ID.
- <yourOrganizationID>: Replace the parameter with the organization ID.
- <yourInstanceID>: Replace the parameter with the instance ID.

```
package main
import (
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk"
    "fmt"
)
func main() {
    client, err := sdk.NewClientWithAccessKey(
        "<yourRegionID>", //Replace the parameter with the region ID.
        "<yourAccessKeyID>", //Replace the parameter with the AccessKey ID.
        "<yourAccessKeySecret>") //Replace the parameter with your AccessKey secret.
    if err != nil {
        panic(err)
    }
    request := requests.NewCommonRequest()
    request.Method = "POST"
    request.Domain = "<vpc.aliyuncs.com>" // Replace the parameter with the endpoint of the
service.
    request.Product = "Vpc"
    request.Version = "2016-04-28"
    // This is an RPC API operation. Therefore, the ApiName(Action) parameter must be speci
fied.
    request.ApiName = "DescribeEipAddresses"
    // Configure service-related parameters.
    request.QueryParams["PageNumber"] = "1"
    request.QueryParams["PageSize"] = "30"
    /*
    When you use STS AccessKey credentials to call an RPC API operation, you must add the
SecurityToken field in the request parameters.
    Format:
    request.QueryParams["SecurityToken"]="<yourSecurityToken>"
    Specify your security token.
    */
    request.Headers["x-acs-regionid"] = "<yourRegionID>" // Optional. Specify your region I
D. 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 t
he organization ID.
    // request.Headers["x-acs-instanceid"] = "<yourInstanceID>" // Optional. Specify the in
stance 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 table lists API operations available for use in Elastic IP Address (EIP).

API	Description
AllocateEipAddress	Applies for an EIP.
AllocateEipAddressPro	Applies for a specified EIP.
AssociateEipAddress	Associates an EIP with a cloud resource.
AllocateEipSegmentAddress	Applies for a contiguous EIP group.
DescribeEipSegment	Queries contiguous EIP groups.
ReleaseEipSegmentAddress	Releases a contiguous EIP group.
ModifyEipAddressAttribute	Modifies the name, description, and bandwidth limit of a specified EIP.
DescribeEipAddresses	Queries the EIPs in a specified region.
UnassociateEipAddress	Disassociates an EIP from a cloud resource.
ReleaseEipAddress	Releases a specified EIP.
DescribeEipGatewayInfo	Queries the gateway and subnet mask information about a specified EIP.
DescribeEipMonitorData	Queries monitoring information about a specified EIP.
MoveResourceGroup	Changes the resource group to which a specified cloud resource belongs.
DescribeHighDefinitionMonitorLogAttribute	Queries fine-grained monitoring configurations of an EIP.

6.2. Make API requests

6.2.1. Request syntax

To call an Elastic IP Address (EIP) API operation, you must send an HTTP GET request to the endpoint of the EIP 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.

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

The request syntax is as follows:

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

where:

- Endpoint: the endpoint of the API. The endpoint of the EIP 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 [Generate the ASAPI endpoint](#).

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

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

The following example describes how to call the DescribeEipAddresses operation to query EIPs.

 **Note** The following code has been formatted for ease of reading.

```
https://vpc.example.com/?Action=DescribeEipAddresses
&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 EIP API operations as a RAM user. To call the EIP API as a RAM user, you must create and add an authorization policy that grants permissions to call specific API operations.

For more information about the EIP resources and API operations that allow the authorization, see [RAM authentication](#).

6.2.3. Signature method guidelines

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

Elastic IP Address (EIP) 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 logon username and password. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of the user, while the AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential. For more information about how to create an AccessKey pair, see [Obtain an AccessKey pair](#).

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

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

Take DescribeEipAddresses as an example. If the AccessKey ID is `testid` and the AccessKey secret is `testsecret`, the pre-signed request URL is:

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

Perform the following operations to calculate the signature:

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

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeEipAddresses&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2014-05-15
```

2. Calculate the HMAC value of the string to be signed.

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

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. Add the signature string to the request:

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

6.3. RAM authentication

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

EIP resources that allow authorized access

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

Resource type	ARN
EIPs	<code>acs:vpc:\$regionid:\$accountid:eip/\$allocationid</code>
	<code>acs:vpc:\$regionid:\$accountid:eip/*</code>
	<code>acs:vpc:*\$accountid:eip/*</code>
General resources	<code>acs:vpc:\$regionid:\$accountid:*</code>
	<code>acs:vpc:*\$accountid:*</code>

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

EIP API operations that allow authorized access

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

API	ARN
AllocateEipAddress	<code>acs:vpc:\$regionid:\$accountid:eip/*</code>
AllocateEipAddressPro	<code>acs:vpc:\$regionid:\$accountid:eip/*</code>
AssociateEipAddress	<code>acs:vpc:\$regionid:\$accountid:eip/*</code>
	Associate an Elastic Compute Service (ECS) instance
	<code>acs:vpc:\$regionid:\$accountid:eip/\$allocationid</code> <code>acs:ecs:\$regionid:\$accountid:instance/\$instanceid</code>
DescribeEipAddresses	<code>acs:vpc:\$regionid:\$accountid:eip/*</code>
UnassociateEipAddress	Associate an ECS instance
	<code>acs:vpc:\$regionid:\$accountid:eip/\$allocationid</code> <code>acs:ecs:\$regionid:\$accountid:instance/\$instanceid</code>
ReleaseEipAddress	<code>acs:vpc:\$regionid:\$accountid:eip/\$allocationid</code>
DescribeEipMonitorData	<code>acs:vpc:\$regionid:\$accountid:eip/\$allocationid</code>
	<code>acs:ecs:\$regionid:\$accountid:instance/\$instanceid</code>

6.4. Common parameters

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

Common request parameters

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

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The format in which to return the response. Valid values: <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> . Set the value to <i>2016-04-28</i> .
AccessKeyId	String	Yes	The AccessKey ID provided to you by Apsara Stack.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to <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, 2013-01-10T12:00:00Z.
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.

Examples

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

Common response parameters

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

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

- XML format

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

- JSON format

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

6.5. Elastic IP addresses

6.5.1. AllocateEipAddress

Applies for an elastic IP address (EIP).

Description

After you call this operation, the system randomly allocates an EIP that is in the **Available** state in the specified region. EIPs support only the ICMP, TCP, and UDP transport layer protocols. The IGMP and SCTP protocols are not supported.

Request parameters

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

Parameter	Type	Required	Example	Description
Action	String	Yes	AllocateEipAddress	The operation that you want to perform. Set the value to AllocateEipAddress .
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region where you want to apply for an EIP. You can call the <code>DescribeRegions</code> operation to query region IDs.
Bandwidth	String	No	1	The bandwidth limit of the EIP. Valid values: 1 to 200 . Unit: Mbit/s. Default value: 1 .
Period	Integer	No	1	The subscription duration of the EIP. When PricingCycle is set to Month , Period can be set from 1 to 9 . When PricingCycle is set to Year , Period can be set from 1 to 3 . This parameter is required when InstanceChargeType is set to PrePaid . When InstanceChargeType is set to PostPaid , ignore this parameter.  Note This parameter is unavailable for EIPs that are purchased on the Alibaba Cloud International site.
ISP	String	No	BGP	The line type. Default value: BGP . - If your account is in the single-path BGP whitelist, you can set the parameter to ChinaTelecom, ChinaUnicom, or ChinaMobile. - This parameter is required if your workloads are deployed in the China East 1 Finance region. In this case, set the value to BGP_FinanceCloud.
ActivityId	Long	No	111111	The promotion code. You can leave this parameter empty.

Parameter	Type	Required	Example	Description
Netmode	String	No	public	The type of network. Set the value to public (Internet).
AutoPay	Boolean	No	false	Specifies whether to enable automatic payment. Valid values: false: disables automatic payment. After an order is generated, you must go to the order center to complete the payment. true: enables automatic payment. After an order is generated, the system automatically deducts fees from your account balance to pay for the order. This parameter is required when InstanceChargeType is set to PrePaid. When InstanceChargeType is set to PostPaid, this parameter is not required.  Note This parameter is unavailable for EIPs that are purchased on the Alibaba Cloud International site.
PricingCycle	String	No	Month	The billing cycle of the subscription EIP. Valid values: Month: billed on a monthly basis. This is the default value. Year: billed on an annual basis. This parameter is required when InstanceChargeType is set to PrePaid. When InstanceChargeType is set to PostPaid, this parameter is not required.  Note This parameter is unavailable for EIPs that are purchased on the Alibaba Cloud International site.

Parameter	Type	Required	Example	Description
InstanceChargeType	String	No	PostPaid	The billing method of the EIP. Valid values: PrePaid: subscription. PostPaid: pay-as-you-go. This is the default value. When InstanceChargeType is set to PrePaid, you must set InternetChargeType to PayByBandwidth. When InstanceChargeType is set to PostPaid, you can set InternetChargeType to PayByBandwidth or PayByTraffic.  Note If you want to purchase an EIP from the Alibaba Cloud International site, you must set this parameter to PostPaid (pay-as-you-go).
InternetChargeType	String	No	PayByTraffic	The metering method of the EIP. Valid values: PayByBandwidth: pay-by-bandwidth. This is the default value. PayByTraffic: pay-by-data-transfer. When InstanceChargeType is set to PrePaid, InternetChargeType must be set to PayByBandwidth. When InstanceChargeType is set to PostPaid, InternetChargeType can be set to PayByBandwidth or PayByTraffic.
ResourceGroupId	String	No	rg-acfmxazffggs**	The ID of the enterprise resource group.

Parameter	Type	Required	Example	Description
ClientToken	String	No	0c593ea1-3bea-11e9-b96b-88e9fe637760	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 ensure that it is unique among different requests. ClientToken can contain only ASCII characters and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Example	Description
EipAddress	String	10.XX.XX.78	The allocated EIP.
AllocationId	String	eip-25877c70gddh****	The ID of the EIP.
OrderId	Long	10	The order number. This parameter is returned only when InstanceChargeType is set to PrePaid .
RequestId	String	4EC47282-1B74-4534-BD0E-403F3EE64CAF	The ID of the request.
ResourceGroupId	String	rg-acfmxazfdgdg****	The ID of the enterprise resource group.

Examples

Sample requests

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

Sample success responses

XML format

```
<AllocateEipAddressResponse>
  <ResourceGroupId>rg-acfmxazfdgdg****</ResourceGroupId>
  <RequestId>4EC47282-1B74-4534-BD0E-403F3EE64CAF</RequestId>
  <AllocationId>eip-25877c70gddh****</AllocationId>
  <EipAddress>10.XX.XX.78</EipAddress>
  <OrderId>10</OrderId>
</AllocateEipAddressResponse>
```

JSON format

```
{
  "AllocateEipAddressResponse": {
    "ResourceGroupId": "rg-acfmxazfdgdg****",
    "RequestId": "4EC47282-1B74-4534-BD0E-403F3EE64CAF",
    "AllocationId": "eip-25877c70gddh****",
    "EipAddress": "10.XX.XX.78",
    "OrderId": 10
  }
}
```

Error codes

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. Apply for permissions and try again.
400	QuotaExceeded.Eip	Elastic IP address quota exceeded	The error message returned because the number of EIPs reaches the quota. You can submit a ticket to request a quota increase. We recommend that you use NAT gateways.
400	InvalidParameter	Specified value of "InternetChargeType" is not valid	The error message returned because InternetChargeType is set to an invalid value.
400	InvalidParameter	Specified value of "Bandwidth" is not valid.	The error message returned because the specified bandwidth limit is invalid.
400	InsufficientBalance	Your account does not have enough balance.	The error message returned because the balance in your account is insufficient. Top up your account and try again.
400	QuotaExceeded.Eip	Elastic IP address quota exceeded.	The error message returned because the number of EIPs reaches the quota. You can submit a ticket to request a quota increase. We recommend that you use NAT gateways.
400	ReserveIpFail	Reserve eip failed.	The error message returned because the system failed to reserve the EIP.

HttpCode	Error code	Error message	Description
400	InvalidRegion.NotSupport	The specified region does not support.	The error message returned because the specified region does not support this operation.
400	InvalidResourceGroupId	The specified ResourceGroupId does not exist.	The error message returned because the specified resource group ID does not exist.
409	OperationConflict	Request was denied due to conflict with a previous request.	The error message returned because a request conflict occurs. Try again later or submit a ticket to report the problem.

6.5.2. AllocateEipAddressPro

Applies for a specified EIP.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AllocateEipAddressPro	The operation that you want to perform. Set the value to AllocateEipAddressPro .
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the specified EIP for which you want to apply. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
IpAddress	String	No	12.XX.XX.23	The IP address of the specified EIP. Specify IpAddress or InstanceId . If you leave both parameters empty, the system randomly allocates an EIP.
InstanceId	String	No	eip-25877c70gddh***	The ID of the specified EIP. Specify IpAddress or InstanceId . If you leave both parameters empty, the system randomly allocates an EIP.
Bandwidth	String	No	5	The bandwidth limit of the specified EIP. Unit: Mbit/s. Default value: 1.

Parameter	Type	Required	Example	Description
Period	Integer	No	1	The subscription duration of the EIP. If PricingCycle is set to Month, set Period to a value from 1 to 9. If PricingCycle is set to Year, set Period to a value from 1 to 3. This parameter is required when InstanceChargeType is set to PrePaid. Leave this parameter empty when InstanceChargeType is set to PostPaid.
ISP	String	No	BGP	The line type. Default value: BGP. If your account is in the single-path BGP whitelist, you can set the parameter to ChinaTelecom, ChinaUnicom, or ChinaMobile. This parameter is required if your workloads are deployed in the China East 1 Finance region. In this case, set the value to BGP_FinanceCloud.
Netmode	String	No	public	The type of network. Set the value to public (Internet). Default value: public (Internet).
Name	String	No	Test123	The name of the EIP. The name must be 2 to 128 characters in length and can contain digits, periods (.), underscores (_), and hyphens (-). It must start with a letter. It cannot start with <code>http://</code> or <code>https://</code>.
Description	String	No	abc	The description of the EIP. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with <code>http://</code> or <code>https://</code>.

Parameter	Type	Required	Example	Description
AutoPay	Boolean	No	true	Specifies whether to enable automatic payment. Valid values: false: disables automatic payment. After an order is generated, you must go to the Order Center to make the payment. true: enables automatic payment. Payments are automatically made. This parameter is required when InstanceChargeType is set to PrePaid. Leave this parameter empty when InstanceChargeType is set to PostPaid.
PricingCycle	String	No	Month	The billing cycle of the subscription EIP. Valid values: • Month (default): The instance is billed on a monthly basis. • Year: The instance is billed on an annual basis. This parameter is required if InstanceChargeType is set to PrePaid. This parameter is optional if InstanceChargeType is set to PostPaid.
InstanceChargeType	String	No	PostPaid	The billing method of the specified EIP. Valid values: PrePaid: subscription PostPaid (default): pay-as-you-go If InstanceChargeType is set to PrePaid, you must set InternetChargeType to PayByBandwidth. If InstanceChargeType is set to PostPaid, you can set InternetChargeType to PayByBandwidth or PayByTraffic.

Parameter	Type	Required	Example	Description
InternetChargeType	String	No	PayByBandwidth	The metering method of the specified EIP. Valid values: PayByBandwidth (default): pay-by-bandwidth PayByTraffic: pay-by-data-transfer If InstanceChargeType is set to PrePaid, you must set InternetChargeType to PayByBandwidth. If InstanceChargeType is set to PostPaid, you can set InternetChargeType to PayByBandwidth or PayByTraffic.
ResourceGroupId	String	No	rg-resourcegroup***	The ID of the resource group to which the EIP belongs.
ClientToken	String	No	0c593ea1-3bea-11e9-b96b-88e9fe637760	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. ClientToken can contain only ASCII characters and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Example	Description
AllocationId	String	eip-25877c70gddh****	The ID of the specified EIP.
EipAddress	String	12.XX.XX.23	The IP address of the specified EIP.
OrderId	Long	20190000	the ID of the order.
RequestId	String	4EC47282-1B74-4534-BD0E-403F3EE64CAF	The ID of the request.
ResourceGroupId	String	rg-resourcegroup****	The ID of the resource group.

Examples

Sample requests

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

Sample success responses

XML format

```
<AllocateEipAddressProResponse>
  <ResourceGroupId>rg-resourcegroup****</ResourceGroupId>
  <RequestId>4EC47282-1B74-4534-BD0E-403F3EE64CAF</RequestId>
  <AllocationId>eip-25877c70gddh****</AllocationId>
  <EipAddress>12.XX.XX.23</EipAddress>
  <OrderId>20190000</OrderId>
</AllocateEipAddressProResponse>
```

JSON format

```
{
  "ResourceGroupId": "rg-resourcegroup****",
  "RequestId": "4EC47282-1B74-4534-BD0E-403F3EE64CAF",
  "AllocationId": "eip-25877c70gddh****",
  "EipAddress": "12.XX.XX.23",
  "OrderId": 20190000
}
```

Error codes

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. Apply for permissions and try again.
400	QuotaExceeded.Eip	Elastic IP address quota exceeded	The error message returned because the number of EIPs reaches the quota. You can submit a ticket to request a quota increase. We recommend that you use NAT gateways.
400	InvalidParameter	Specified value of "InternetChargeType" is not valid	The error message returned because InternetChargeType is set to an invalid value.
400	InvalidParameter	Specified value of "Bandwidth" is not valid.	The error message returned because the specified bandwidth limit is invalid.

HttpCode	Error code	Error message	Description
400	InsufficientBalance	Your account does not have enough balance.	The error message returned because the balance in your account is insufficient. Top up your account and try again.
400	QuotaExceeded.Eip	Elastic IP address quota exceeded.	The error message returned because the number of EIPs reaches the quota. You can submit a ticket to request a quota increase. We recommend that you use NAT gateways.
400	ReserveIpFail	Reserve eip failed.	The error message returned because the system failed to reserve the EIP.
400	InvalidRegion.NotSupport	The specified region does not support.	The error message returned because the specified region does not support this operation.
400	InvalidResourceGroupId	The specified ResourceGroupId does not exist.	The error message returned because the specified resource group ID does not exist.

6.5.3. AssociateEipAddress

Associates an elastic IP address (EIP) with an instance in the same region.

Description

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

- You can associate an EIP with an Elastic Compute Service (ECS) instance, a Server Load Balancer (SLB) instance, a secondary elastic network interface (ENI), or a NAT gateway that is deployed in a virtual private cloud (VPC). The EIP and the instance with which you want to associate the EIP must belong to the same region.
- To associate an EIP with a NAT gateway, make sure that no NAT service plan that was purchased before November 3, 2017 exists in your account.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AssociateEipAddress	The operation that you want to perform. Valid values: AssociateEipAddress .
AllocationId	String	Yes	eip-2zeerraiwb7ujxsdc****	The ID of the EIP that you want to associate with an instance.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	i-2zebb08phyczza-we****	The ID of the instance with which you want to associate the EIP. NAT gateways, SLB instances, ECS instances, secondary ENIs, and high-availability virtual IP addresses (HAVIPs) are supported.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region to which the EIP belongs.
InstanceType	String	No	EcsInstance	The type of instance with which you want to associate the EIP. Valid values: Nat : NAT Gateway. SlbInstance : SLB SLB. EcsInstance : ECS instances. NetworkInterface : auxiliary Elastic Network Interface. HaVip : High-availability virtual IP addresses.
InstanceRegionId	String	No	cn-hangzhou	The ID of the region where the instance to be associated with the EIP is deployed.  Note This parameter is required only when the EIP is associated with a shared-bandwidth Global Accelerator (GA) instance.
PrivateIpAddress	String	No	192.1.XX.XX	An IP address that belongs to the CIDR block of a vSwitch. If you do not set this parameter, the system allocates a private IP address based on the VPC ID and vSwitch ID.

Parameter	Type	Required	Example	Description
Mode	String	No	NAT	The binding mode. Valid values: • NAT : NAT mode (normal mode). • MULTI_BINDED : The multi-EIP network interface controller visible mode. • BINDED : The visible mode of the EIP network interface controller. Only InstanceType Configure as NetworkInterface this parameter is required.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-001sdfg	Guaranteed request idempotence. You can use the client to generate the value, but you must ensure that it is unique among different requests. <code>ClientToken</code> Only ASCII characters are supported and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C0FD0EED-F90D-4479-803D-DD62335357E5	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AssociateEipAddress
&AllocationId=eip-2zeerraiwb7ujsxdc****
&InstanceId=i-2zebb08phyczzawe****
&<Public request parameters>
```

Sample success responses

XML format

```
<AssociateEipAddressResponse>
  <RequestId>C0FD0EED-F90D-4479-803D-DD62335357E5</RequestId>
</AssociateEipAddressResponse>
```

JSON format

```
{
  "RequestId": "C0FD0EED-F90D-4479-803D-DD62335357E5"
}
```

Error codes

HttpCode	Error code	Error message	Description
400	InvalidAssociation.Duplicated	Specified instance already is associated.	The error message returned because an EIP or a GA instance is already associated with the specified instance. You must disassociate the EIP or GA instance from the specified instance before you can perform the operation.
400	OperationDenied	Specified instance is not in VPC.	The error message returned because the specified instance does not exist in the VPC.
400	InvalidParameter.Mismatch	Specified elastic IP address and ECS instance are not in the same region.	The error message returned because the specified EIP and ECS instance do not belong to the same region.
400	IncorrectEipStatus	Current elastic IP status does not support this operation	The error message returned because the state of the EIP does not support the operation.
404	InvalidInstanceId.NotFound	Specified instance does not exist.	The error message returned because the specified instance does not exist. Check whether the ID is valid.
400	IncorrectInstanceStatus	Current instance status does not support this operation.	The error message returned because this operation cannot be performed while the instance is in the current state.
400	InvalidInstanceType.ValueNotSupported	The specified value of InstanceType is not supported.	The error message returned because InstanceType is set to an invalid value.
400	IncorrectHaVipStatus	HaVip can be operated by this action only when it's status is Available or InUse.	The error message returned because the state of the HAVIP does not support the operation. You can perform the operation only when the HAVIP is in the Available or InUse state.
400	InvalidParameter	The specified parameter is not valid.	The error message returned because the specified value of the parameter is invalid.

HttpCode	Error code	Error message	Description
400	OperationDenied	Eip of default vpc not allow this operation	The error message returned because the operation is not supported by EIPs in the default VPC.
400	Forbidden	The eip instance owner error	The error message returned because you are unauthorized to perform the operation on the EIP.
400	InvalidBindingStatus	The eip binding status invalid.	The error message returned because the EIP is in an invalid state.
400	BIND_INSTANCE_HAVING_PORT_MAP_OR_BIND_EIP	The instance may have portMap or already bind eip.	The error message returned because a port forwarding rule is configured for the ECS instance. Delete the port forwarding rule and try again.
400	BIND_INSTANCE_OWNER_ERROR	Cannot operate the eip.	The error message returned because you are unauthorized to manage the specified EIP.
404	InvalidAllocationId.NotFound	Specified allocation ID is not found	The error message returned because the specified EIP does not exist. Check whether the value of the parameter is valid.
400	InvalidParams.NotFound	instance not found	The error message returned because the specified instance does not exist.
503	ServiceUnavailable	The request has failed due to a temporary failure of the server.	The error message returned because the request failed due to a temporary malfunction of the server.

6.5.4. AllocateEipSegmentAddress

Applies for a contiguous elastic IP address (EIP) group.

Request parameters

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

Parameter	Type	Required	Example	Description
EipMask	String	Yes	28	The subnet mask length for the contiguous EIP group. Valid values: • 28: applies for 16 contiguous EIPs in each call. • 27: applies for 32 contiguous EIPs in each call. • 26: applies for 64 contiguous EIPs in each call. • 25: applies for 128 contiguous EIPs in each call. • 24: applies for 256 contiguous EIPs in each call.  Note The number of contiguous EIPs allocated by the system may be less than the requested number because one, three, or four EIPs may be reserved.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the contiguous EIP group. You can call the DescribeRegions operation to query the most recent region list.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-001sdfg	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.  Note If you do not set this parameter, the system automatically uses RequestId as ClientToken. RequestId of each API request may be different.
Bandwidth	String	No	5	The maximum bandwidth of the EIP. Unit: Mbit/s. Default value: 5.

Parameter	Type	Required	Example	Description
Netmode	String	No	public	The network type. Valid values: public (default): Internet. After the contiguous EIP group is associated with a cloud resource, the cloud resource can communicate with the Internet by using the EIPs in the contiguous EIP group. hybrid: hybrid cloud. After the contiguous EIP group is associated with a cloud resource, the cloud resource can communicate with a hybrid cloud by using the EIPs in the contiguous EIP group.  Note This network type is available only to users who are included in the whitelist. To use this network type, contact your business manager.
InternetChargeType	String	No	PayByBandwidth	The metering method of the contiguous EIP group. Valid values: PayByBandwidth (default): pay-by-bandwidth PayByTraffic: pay-by-data-transfer  Note If the Netmode parameter is set to hybrid, you can set InternetChargeType only to PayByBandwidth.
ResourceGroupId	String	No	rg-bp67acfmxazb4ph****	The ID of the resource group to which the contiguous EIP group belongs.
Isp	String	No	BGP	The line type. Valid values: BGP: BGP (Multi-ISP) BGP_PRO: BGP (Multi-ISP) Pro

Response parameters

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

Parameter	Type	Example	Description
EipSegmentInstanceId	String	eipsg-2zett8ba055tbsxme****	The ID of the contiguous EIP group.
OrderId	Long	20190000	The ID of the order.
RequestId	String	F7A6301A-64BA-41EC-8284-8F4838C15D1F	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AllocateEipSegmentAddress
&EipMask=28
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<AllocateEipSegmentAddress>
  <EipSegmentInstanceId>eipsg-2zett8ba055tbsxme****</EipSegmentInstanceId>
  <RequestId>F7A6301A-64BA-41EC-8284-8F4838C15D1F</RequestId>
  <OrderId>20190000</OrderId>
</AllocateEipSegmentAddress>
```

JSON format

```
{
  "EipSegmentInstanceId": "eipsg-2zett8ba055tbsxme****",
  "RequestId": "F7A6301A-64BA-41EC-8284-8F4838C15D1F",
  "OrderId": 20190000
}
```

Error code

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 this operation on the specified resource. Apply for the required permissions and try again.

HttpCode	Error code	Error message	Description
400	InvalidParameter	Specified value of "Bandwidth" is not valid.	The error message returned because the specified bandwidth value is invalid.
400	InsufficientBalance	Your account does not have enough balance.	The error message returned because you do not have sufficient balance within your Apsara Stack tenant account. Top up your Apsara Stack tenant account and try again.
400	QuotaExceeded.Eip	Elastic IP address quota exceeded.	The error message returned because the number of EIPs has reached the upper limit. We recommend that you use NAT gateways if you want to use more EIPs.
400	ReserveIpFail	Reserve eip failed.	The error message returned because the system failed to reserve the specified EIP.
400	InvalidRegion.NotSupport	The specified region does not support.	The error message returned because the operation is not supported in the specified region.
400	InvalidResourceGroupId	The specified ResourceGroupId does not exist.	The error message returned because the specified resource group ID is invalid.
409	OperationConflict	Request was denied due to conflict with a previous request.	The error message returned because your request is conflicting with another request. Try again later.
400	ORDER.QUANTITY_INVALID	User quota has exceeded the limit.	The error message returned because the number of EIPs that you have created has reached the upper limit. Go to the Quota Management page to request a quota increase.
500	OrderError.EIP	The Account failed to create order.	The error message returned because the system failed to generate the order.

6.5.5. DescribeEipSegment

Queries contiguous elastic IP address (EIP) groups.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEipSegment	The operation that you want to perform. Set the value to DescribeEipSegment .
RegionId	String	Yes	cn-qingdao-env66-d01	The ID of the region to which the contiguous EIP group belongs. You can call the DescribeRegions operation to query the most recent region list.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-00****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length. Note If you do not set this parameter, the system automatically uses RequestId as ClientToken . RequestId of each API request may be different.
SegmentInstanceId	String	No	eipsg-2zett8ba055tbsxme****	The ID of the contiguous EIP group that you want to query.
PageNumber	Integer	No	1	The page 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
EipSegments	Array of EipSegment		The details of the contiguous EIP groups.
EipSegment			

Parameter	Type	Example	Description
CreationTime	String	2021-03-06T12:30:07Z	The time when the contiguous EIP group was created. The time is in the <code>ISO 8601</code> standard in the yyyy-MM-ddTHH:mm:ssZ format. The time is in UTC+0.
Description	String	MyEipSegment	The description of the contiguous EIP group.
InstanceId	String	eipsg-2zett8ba055tbsxme****	The ID of the contiguous EIP group.
IpCount	String	28	The number of EIPs in the contiguous EIP group.
Name	String	MyEipSegment	The name of the contiguous EIP group.
RegionId	String	cn-qingdao-env66-d01	The ID of the region to which the contiguous EIP group belongs.
Segment	String	161.XX.XX.0/28	The CIDR block and subnet mask of the contiguous EIP group.
Status	String	Allocated	The status of the contiguous EIP group. Valid values: Allocating: being allocated Allocated: allocated Releasing: being released Released: released
PageNumber	Integer	2	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	F7A6301A-64BA-41EC-8284-8F4838C15D1F	The ID of the request.
TotalCount	Integer	1	The number of entries returned.

Examples

Sample requests

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

Sample success responses

XML format

```
<DescribeEipSegmentResponse>
  <EipSegments>
    <Status>Allocated</Status>
    <Description>MyEipSegment</Description>
    <IpCount>28</IpCount>
    <InstanceId>eipsg-2zett8ba055tbsxme****</InstanceId>
    <CreationTime>2021-03-06T12:30:07Z</CreationTime>
    <RegionId>cn-qingdao-env66-d01</RegionId>
    <Segment>161.XX.XX.0/28</Segment>
    <Name>MyEipSegment</Name>
  </EipSegments>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>F7A6301A-64BA-41EC-8284-8F4838C15D1F</RequestId>
  <PageNumber>2</PageNumber>
</DescribeEipSegmentResponse>
```

JSON format

```
{
  "EipSegments": {
    "Status": "Allocated",
    "Description": "MyEipSegment",
    "IpCount": 28,
    "InstanceId": "eipsg-2zett8ba055tbsxme****",
    "CreationTime": "2021-03-06T12:30:07Z",
    "RegionId": "cn-qingdao-env66-d01",
    "Segment": "161.XX.XX.0/28",
    "Name": "MyEipSegment"
  },
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "F7A6301A-64BA-41EC-8284-8F4838C15D1F",
  "PageNumber": 2
}
```

6.5.6. ReleaseEipSegmentAddress

Releases contiguous elastic IP addresses (EIPs).

Description

You can call this operation to release all EIPs in a group of contiguous EIPs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ReleaseEipSegmentAddress	The operation that you want to perform. Set the value to ReleaseEipSegmentAddress .
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the contiguous EIPs. You can call the DescribeRegions operation to query the most recent region list.
SegmentInstanceId	String	Yes	eipsg-2zett8ba055tbsxme****	The ID of the group to which the contiguous EIPs to be released belongs. The system releases all EIPs in the group.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-00****	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must make sure that it is unique among different requests. The token can contain only ASCII characters and cannot exceed 64 characters in length.  Note If you do not set this parameter, the system automatically uses RequestId as ClientToken. RequestId of each API request may be different.

Response parameters

Parameter	Type	Example	Description
RequestId	String	F7A6301A-64BA-41EC-8284-8F4838C15D1F	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ReleaseEipSegmentAddress
&RegionId=cn-qingdao-env17-d01
&SegmentInstanceId=eipsg-2zett8ba055tbsxme****
&<Common request parameters>
```

Sample success responses

XML format

```
<ReleaseEipSegmentAddressResponse>
  <RequestId>F7A6301A-64BA-41EC-8284-8F4838C15D1F</RequestId>
</ReleaseEipSegmentAddressResponse>
```

JSON format

```
{
  "RequestId": "F7A6301A-64BA-41EC-8284-8F4838C15D1F"
}
```

Error codes

HttpCode	Error code	Error message	Description
400	IncorrectEipStatus	Current elastic IP status does not support this operation.	The error message returned because you cannot perform the operation when the specified EIPs are in the current state.
500	InternalError	The request processing has failed due to some unknown error.	The error message returned because an unknown error occurred.
404	Forbidden.RegionNotFound	Specified region is not found during access authentication.	The error message returned because the specified region does not exist. Check whether the specified region ID is valid.
400	Forbidden.ChargeTypesPrepaid	It's forbidden to release a prepaid EIP	The error message returned because you cannot release subscription EIPs.
400	Forbidden	The eip instance owner error	The error message returned because the EIPs do not belong to you. Check whether you are unauthorized to perform the operation on the EIPs.
400	TaskConflict.AssociateGlobalAccelerationInstance	Operate too frequent.	The error message returned because the number of requests that you send exceeds the upper limit.

6.5.7. ModifyEipAddressAttribute

Modifies the name, description, and bandwidth limit of a specified elastic IP address (EIP).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyEipAddressAttribute	The operation that you want to perform. Set the value to ModifyEipAddressAttribute .
AllocationId	String	Yes	eip-2zeerraiwb7uj6i0d****	The ID of the EIP that you want to modify.
Bandwidth	String	No	100	The bandwidth limit of the EIP. Valid values: 1 to 200 . Unit: Mbit/s.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region to which the EIP belongs.
Name	String	No	Test123	The name of the EIP. The name must be 2 to 128 characters in length, and can contain, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter. The name cannot start with <code>http://</code> or <code>https://</code> .
Description	String	No	abc	The description of the EIP. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with <code>http://</code> or <code>https://</code> .

Response parameters

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

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyEipAddressAttribute
&AllocationId=eip-2zeerraiwb7uj6i0d****
&<Common request parameters>
```

Sample success responses

XML format

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

JSON format

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

Error codes

HttpCode	Error code	Error message	Description
400	InsufficientBalance.Eip	Your account does not have enough balance.	The error message returned because the balance in your account is insufficient. Top up your account and try again.
404	InvalidAllocationId.NotFound	Specified allocation ID is not found	The error message returned because the specified EIP does not exist. Check whether the value of the parameter is valid.
400	InvalidParameter	Specified value of "Bandwidth" is not supported.	The error message returned because the specified bandwidth limit is invalid.
500	InternalError	The request processing has failed due to some unknown error.	The error message returned because an unknown error occurred.
400	IncorrectEipStatus	Current elastic IP status does not support this operation.	The error message returned because the state of the EIP does not support this operation.
404	InvalidAllocationId.NotFound	Specified allocation ID is not found..	The error message returned because the specified EIP does not exist. Check whether the value of the parameter is valid.

HttpCode	Error code	Error message	Description
400	InvalidParameter	The parameter is invalid.	The error message returned because the parameter is set to an invalid value.
404	Forbidden.RegionNotFound	Specified region is not found during access authentication.	The error message returned because the specified region does not exist. Check whether the specified region ID is valid.

6.5.8. DescribeEipAddresses

Queries elastic IP addresses (EIPs) created in a specific region.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEipAddresses	The operation that you want to perform. Set the value to DescribeEipAddresses .
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the EIP. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
Tag.N.Key	String	No	TestKey	The key of tag N of the instance that you want to query. Valid values of N: 1 to 20.
Tag.N.Value	String	No	TestValue	The value of tag N of the instance that you want to query. Valid values of N: 1 to 20.
IncludeReservationData	Boolean	No	true	Specify whether to return data of orders that have not taken effect. Valid values: false: does not return data of orders that have not taken effect. This is the default value. true: returns data of orders that have not taken effect.

Parameter	Type	Required	Example	Description
Status	String	No	Available	The status of the EIP. Valid values: • Associating: The EIP is being associated with an instance. • Unassociating: The EIP is being disassociated from an instance. • InUse: The EIP is associated with an instance. • Available: The EIP is available.
EipAddress	String	No	116.xx.xx.28	The IP address of the EIP that you want to query. You can enter up to 50 IP addresses of EIPs. Separate multiple IP addresses with commas (,).  Note If both the EipAddress and AllocationId parameters are set, you can enter up to 50 IP addresses of EIPs in EipAddress, and enter up to 50 IDs of EIPs in AllocationId.
AllocationId	String	No	eip-2zeerraiwb7ujxscd****	The ID of the EIP that you want to query. You can enter up to 50 IDs of EIPs. Separate multiple IDs with commas (,).  Note If both the EipAddress and AllocationId parameters are set, you can enter up to 50 IDs of EIPs in AllocationId, and enter up to 50 IP addresses of EIPs in EipAddress.
SegmentInstanceId	String	No	eipsg-t4nr90yik5oy38xdy****	The IDs of contiguous EIPs.
ResourceGroupId	String	No	rg-acfmxazb4pcdvf***	The ID of the resource group to which the EIPs belong.

Parameter	Type	Required	Example	Description
PageNumber	Integer	No	10	The number of the page to return. Default value: 1 .
PageSize	Integer	No	10	The number of entries to return on each page. Maximum value: 100 . Default value: 10 .
ISP	String	No	BGP	The Internet service provider (ISP). Set the value to BGP .
Filter.1.Key	String	No	CreationStartTime	The filter key used to query resources. Set the value to CreationStartTime , which indicates the time when the system started to create the resource.
Filter.2.Key	String	No	CreationEndTime	The filter key used to query resources. Set the value to CreationEndTime , which indicates the time when the system completed creating the resource.
Filter.1.Value	String	No	2018-01-22T09:12Z	The filter value used to query resources. Specify the time in the ISO 8601 standard in <code>YYYY-MM-DDThh:mmZ</code> format. The time must be in UTC.
Filter.2.Value	String	No	2018-01-22T09:15Z	The filter value used to query resources. Specify the time in the ISO 8601 standard in <code>YYYY-MM-DDThh:mmZ</code> format. The time must be in UTC.
LockReason	String	No	financial	The reason why the EIP is locked. Valid values: financial: The EIP is locked due to overdue payments. security: The EIP is locked for security reasons.

Parameter	Type	Required	Example	Description
AssociatedInstanceType	String	No	EcsInstance	The type of the cloud resource with which you want to associate the EIP. Valid values: EcsInstance: an Elastic Compute Service (ECS) instance in a virtual private cloud (VPC). This is the default value. SlbInstance: a Server Load Balancer (SLB) instance in a VPC. Nat: a NAT gateway. HaVip: a high-availability virtual IP address (HAVIP). NetworkInterface: a secondary elastic network interface (ENI). You can associate only one EIP with each ECS instance, SLB instance, or HAVIP. You can associate multiple EIPs with each NAT gateway. The number of EIPs that can be associated with a secondary ENI depends on the EIP association mode.
AssociatedInstanceId	String	No	i-2zebb08phyccdvf****	The ID of the cloud resource with which the EIP is associated.
ChargeType	String	No	None	The billing method of the EIP. Valid values: PostPaid: pay-as-you-go PrePaid: subscription
DryRun	Boolean	No	false	Specifies whether to precheck only this request. Valid values: true: prechecks the request only. EIPs are not queried. The system checks the required parameters, request syntax, and service limits. If the request fails the precheck, the corresponding error message is returned. If the request passes the precheck, the <code>DryRunOperation</code> error code is returned. false: prechecks the request. This is the default value. After the request passes the check, a 2xx HTTP status code is returned and EIPs are queried.

Response parameters

Parameter	Type	Example	Description
EipAddresses	Array of EipAddress		The details about the EIP.
EipAddress			
AllocationId	String	eip-2zeerraiwb7ujcdvf**	The ID of the EIP.
AllocationTime	String	2019-04-23T01:37:38Z	The time when the EIP was created.
AvailableRegions	List	cn-east-hangzhou-01	The ID of the region to which the EIP belongs.
Bandwidth	String	5	The bandwidth limit of the EIP. Unit: Mbit/s.
BandwidthPackageBandwidth	String	50	The bandwidth of the EIP bandwidth plan. Unit: Mbit/s.
BandwidthPackageId	String	cbwp-bp1ego3i4j07ccdvf***	The ID of the EIP bandwidth plan.
BandwidthPackageType	String	CommonBandwidthPackage	The type of the bandwidth. Only CommonBandwidthPackage (EIP Bandwidth Plan) is returned.
ChargeType	String	PostPaid	The billing method of the EIP. PrePaid: subscription PostPaid: pay-as-you-go
DeletionProtection	Boolean	true	Indicates whether deletion protection is enabled. Valid values: true: enabled false: disabled
Description	String	abc	The description of the EIP.
EipBandwidth	String	101	The bandwidth limit of the EIP when it is not associated with an EIP bandwidth plan.

Parameter	Type	Example	Description
ExpiredTime	String	2019-04-29T02:00Z	The expiration date. The time follows the ISO 8601 standard and is displayed in UTC. Format: <code>YYYY-MM-ddTHH:mmZ</code> .
HdMonitorStatus	String	false	Indicates whether fine-grained monitoring is enabled for the EIP. Valid values: false: disabled true: enabled
HasReservationData	String	false	Indicates whether renewal data is included. This parameter returns true only when the IncludeReservationData parameter is set to true and some orders have not taken effect.
ISP	String	BGP	The ISP.
InstanceId	String	i-bp15zckdt37cdvf***	The ID of the instance with which the EIP is associated.
InstanceRegionId	String	cn-east-hangzhou-01	The region ID of the associated resource.
InstanceType	String	EcsInstance	The type of the instance associated with the EIP. Valid values: EcsInstance: an ECS instance in a VPC. SlbInstance: an SLB instance in a VPC. Nat: a NAT gateway. HaVip: an HAVIP. NetworkInterface: a secondary ENI.
InternetChargeType	String	PayByBandwidth	The metering method of the EIP. Valid values: PayByBandwidth: pay-by-bandwidth PayByTraffic: pay-by-data-transfer
IpAddress	String	101.xx.xx.36	The IP address of the EIP.

Parameter	Type	Example	Description
Mode	String	NAT	The association mode. Valid values: NAT (default): the standard NAT mode MULTI_BINDED: multi-EIP-to-ENI mode BINDED: cut-through mode This parameter is returned only when InstanceType is set to NetworkInterface.
Name	String	test	The name of the EIP.
Netmode	String	public	The type of network. The value public (Internet) is returned.
OperationLocks	Array of LockReason		The details about the locked EIP.
LockReason			
LockReason	String	financial	The reason why the EIP is locked. Valid values: financial: The EIP is locked due to overdue payments. security: The EIP is locked for security reasons.
PrivateIpAddress	String	192.1.XX.XX	An IP address in the CIDR block of the vSwitch.
RegionId	String	cn-east-hangzhou-01	The ID of the region to which the EIP belongs.
ReservationActiveTime	String	2019-03-11T16:00:00Z	The time when the renewal takes effect.
ReservationBandwidth	String	12	The bandwidth after the renewal takes effect.
ReservationInternetChargeType	String	PayByBandwidth	The metering method of the renewal. Valid values: PayByBandwidth: pay-by-bandwidth PayByTraffic: pay-by-data-transfer

Parameter	Type	Example	Description
ReservationOrderType	String	RENEWCHANGE	The type of the renewal order. Valid values: RENEWCHANGE: upgrade or downgrade TEMP_UPGRADE: temporary upgrade UPGRADE: upgrade
ResourceGroupId	String	rg-acfmxazcdxs****	The ID of the resource group.
SecondLimited	Boolean	false	Indicates whether level-2 throttling is configured. Valid values: true: yes false: no
SegmentInstanceIds	String	eipsg-t4nr90yik5oy38xdyjt h8	The IDs of contiguous EIPs. This value is returned only when contiguous EIPs are specified.
Status	String	Associating	The status of the EIP. Valid values: Associating: The EIP is being associated with an instance. Unassociating: The EIP is being disassociated from an instance. InUse: The EIP is associated with an instance. Available: The EIP is available.
Tags	Array of Tag		The tags used to query resources.
Tag			
Key	String	testX	The filter key used to query resources.
Value	String	testY	The filter value used to query resources.
TotalCount	Integer	10	The total number of entries returned.
PageNumber	Integer	10	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.

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

Examples

Sample requests

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

Sample success responses

`XML` format

```

<DescribeEipAddressesResponse>
  <TotalCount>10</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>4EC47282-1B74-4534-BD0E-403F3EE64CAF</RequestId>
  <EipAddresses>
    <HdMonitorStatus>false</HdMonitorStatus>
    <PrivateIpAddress>192.1.XX.XX</PrivateIpAddress>
    <ResourceGroupId>rg-acfmazcdxs****</ResourceGroupId>
    <AllocationId>eip-2zeerraiwb7ujcdvf****</AllocationId>
    <SecondLimited>false</SecondLimited>
    <Name>test</Name>
    <SegmentInstanceId>eipsg-t4nr90yik5oy38xdyjt8</SegmentInstanceId>
    <ReservationOrderType>RENEWCHANGE</ReservationOrderType>
    <InstanceRegionId>cn-east-hangzhou-01</InstanceRegionId>
    <ExpiredTime>2019-04-29T02:00Z</ExpiredTime>
    <Bandwidth>5</Bandwidth>
    <BandwidthPackageId>cbwp-bplego3i4j07ccdvf****</BandwidthPackageId>
    <ReservationActiveTime>2019-03-11T16:00:00Z</ReservationActiveTime>
    <InstanceType>EcsInstance</InstanceType>
    <ReservationBandwidth>12</ReservationBandwidth>
    <Status>Associating</Status>
    <InstanceId>i-bp15zckdt37cdvf****</InstanceId>
    <Mode>NAT</Mode>
    <ISP>BGP</ISP>
    <HasReservationData>false</HasReservationData>
    <DeletionProtection>true</DeletionProtection>
    <BandwidthPackageType>CommonBandwidthPackage</BandwidthPackageType>
    <BandwidthPackageBandwidth>50</BandwidthPackageBandwidth>
    <ReservationInternetChargeType>PayByBandwidth</ReservationInternetChargeType>
    <InternetChargeType>PayByBandwidth</InternetChargeType>
    <AllocationTime>2019-04-23T01:37:38Z</AllocationTime>
    <Description>abc</Description>
    <EipBandwidth>101</EipBandwidth>
    <Netmode>public</Netmode>
    <ChargeType>PostPaid</ChargeType>
    <IpAddress>101.xx.xx.36</IpAddress>
    <RegionId>cn-east-hangzhou-01</RegionId>
    <OperationLocks>
      <LockReason>financial</LockReason>
    </OperationLocks>
    <Tags>
      <Value>testY</Value>
      <Key>testX</Key>
    </Tags>
    <AvailableRegions>cn-east-hangzhou-01</AvailableRegions>
  </EipAddresses>
  <PageNumber>10</PageNumber>
</DescribeEipAddressesResponse>

```

JSON format

```

{
  "TotalCount": 10,
  "PageSize": 10,
  "RequestId": "4EC47282-1B74-4534-BD0E-403F3EE64CAF",
  "EipAddresses": {
    "HDMonitorStatus": false,
    "PrivateIpAddress": "192.1.XX.XX",
    "ResourceGroupId": "rg-acfmazcdxs****",
    "AllocationId": "eip-2zeerraiwb7ujcdvf****",
    "SecondLimited": false,
    "Name": "test",
    "SegmentInstanceId": "eipsg-t4nr90yik5oy38xdyjt8",
    "ReservationOrderType": "RENEWCHANGE",
    "InstanceRegionId": "cn-east-hangzhou-01",
    "ExpiredTime": "2019-04-29T02:00Z",
    "Bandwidth": 5,
    "BandwidthPackageId": "cbwp-bplego3i4j07ccdvf****",
    "ReservationActiveTime": "2019-03-11T16:00:00Z",
    "InstanceType": "EcsInstance",
    "ReservationBandwidth": 12,
    "Status": "Associating",
    "InstanceId": "i-bp15zckdt37cdvf****",
    "Mode": "NAT",
    "ISP": "BGP",
    "HasReservationData": false,
    "DeletionProtection": true,
    "BandwidthPackageType": "CommonBandwidthPackage",
    "BandwidthPackageBandwidth": 50,
    "ReservationInternetChargeType": "PayByBandwidth",
    "InternetChargeType": "PayByBandwidth",
    "AllocationTime": "2019-04-23T01:37:38Z",
    "Description": "abc",
    "EipBandwidth": 101,
    "Netmode": "public",
    "ChargeType": "PostPaid",
    "IpAddress": "101.xx.xx.36",
    "RegionId": "cn-east-hangzhou-01",
    "OperationLocks": {
      "LockReason": "financial"
    },
    "Tags": {
      "Value": "testY",
      "Key": "testX"
    },
    "AvailableRegions": "cn-east-hangzhou-01"
  },
  "PageNumber": 10
}

```

Error codes

HttpCode	Error code	Error message	Description
404	Forbidden.RegionNotFound	Specified region is not found during access authentication.	The error message returned because the specified region does not exist. Check whether the region is valid.
404	InvalidLockReason.NotFound	The specified LockReason is not found	The error message returned because the reason why the EIP is locked is unknown.
400	InvalidAssociatedInstanceType.ValueNotSupported	The specified value of AssociatedInstanceType is not supported.	The error message returned because AssociatedInstanceType is set to an invalid value. Check whether the value is valid.
400	InvalidChargeType.ValueNotSupported	The specified ChargeType is not supported.	The error message returned because the specified billing method is not supported. Set a supported billing method.
400	InvalidResourceGroupId	The specified ResourceGroupId does not exist.	The error message returned because the specified resource group ID does not exist.
400	OperationUnsupported.ResourceGroupId	ResourceGroup is not supported in this region.	The error message returned because the resource group feature is disabled.

6.5.9. UnassociateEipAddress

Disassociates an elastic IP address (EIP) from an instance.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UnassociateEipAddress	The operation that you want to perform. Set the value to UnassociateEipAddress .
AllocationId	String	Yes	eip-2zeerraiwb7uj6i0d****	The ID of the EIP that you want to disassociate.
InstanceId	String	Yes	i-hp3akk9irt69jad****	The ID of the instance from which you want to disassociate the EIP.

Parameter	Type	Required	Example	Description
Force	Boolean	No	false	Specifies whether to disassociate the EIP from a NAT gateway if a DNAT or SNAT entry is added to the NAT gateway. Valid values: false (default): does not disassociate the EIP from a NAT gateway if a DNAT or SNAT entry is added to the NAT gateway. true: disassociates the EIP from a NAT gateway if a DNAT or SNAT entry is added to the NAT gateway.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region to which the EIP belongs.
InstanceType	String	No	EcsInstance	The type of instance from which you want to disassociate the EIP. Valid values: EcsInstance (default): an Elastic Compute Service (ECS) instance that is deployed in a virtual private cloud (VPC) SlbInstance: a Server Load Balancer (SLB) instance that is deployed in a VPC NetworkInterface: a secondary elastic network interface (ENI) that is deployed in a VPC Nat: a NAT gateway HaVip: a high-availability virtual IP address (HAVIP)
PrivateIpAddress	String	No	192.XX.XX.2	The private IP address of the ECS instance or the secondary ENI from which you want to disassociate the EIP.
ClientToken	String	No	02fb3da4-130e-11e9-8e44-001***	The client token that is used to ensure the idempotence of the request. You can use the client to generate the value, but you must ensure that it is unique among different requests. ClientToken can contain only ASCII characters and cannot exceed 64 characters in length.

Response parameters

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

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=UnassociateEipAddress
&AllocationId=eip-2zeerraiwb7uj6i0d****
&InstanceId=i-hp3akk9irt69jad****
&<Common request parameters>
```

Sample success responses

XML format

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

JSON format

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

Error codes

HttpCode	Error code	Error message	Description
404	InvalidAllocationId.NotFound	Specified allocation ID is not found	The error message returned because the specified EIP does not exist. Check whether the value of the parameter is valid.
400	IncorrectEipStatus	Current elastic IP status does not support this operation.	The error message returned because the state of the EIP does not support this operation.
400	InvalidInstanceId.NotFound	Specified instance does not exist.	The error message returned because the specified instance does not exist. Check whether the specified instance is valid.
400	IncorrectInstanceStatus	The current status of instance does not support this operation.	The error message returned because the state of the instance does not support the operation.

HttpCode	Error code	Error message	Description
400	InvalidInstanceType.ValueNotSupported	The specified value of InstanceType is not supported.	The error message returned because InstanceType is set to an invalid value.
400	IncorrectHaVipStatus	This operation is denied because satus of the specified HaVip is neither Available nor InUse.	The error message returned because you cannot perform the operation when the specified HAVIP is in the Available or InUse state.
400	OperationDenied	Eip of default vpc not allow this operation	The error message returned because EIPs in the default VPC do not support the operation.
404	Forbidden.RegionNotFound	Specified region is not found during access authentication.	The error message returned because the specified region does not exist. Check whether the specified region ID is valid.
400	InvalidParameter	The specified parameter is not valid.	The error message returned because the parameter is set to an invalid value.
400	Forbbiden	The eip instance owener error	The error message returned because you are unauthorized to perform the operation on the EIP.
400	InvalidBindingStatus	The eip binding status invalid.	The error message returned because the binding mode of the EIP is invalid.

6.5.10. ReleaseEipAddress

Releases a specified elastic IP address (EIP).

Description

Before you release an EIP, make sure that the EIP meets the following requirements:

- You can release only EIPs that are in the **Available** state.
- You can release only EIPs that are billed on a pay-as-you-go basis. You cannot release subscription EIPs.

Request parameters

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

Parameter	Type	Required	Example	Description
Action	String	Yes	ReleaseEipAddresses	The operation that you want to perform. Set the value to ReleaseEipAddress .
AllocationId	String	Yes	eip-2zeerraiwb7uj6i0d****	The ID of the EIP that you want to release.
RegionId	String	Yes	cn-qingdao-env17-d01	The ID of the region to which the EIP belongs. You can call the <code>DescribeRegions</code> operation to query region IDs.

Response parameters

Parameter	Type	Example	Description
RequestId	String	748C38F6-9A3D-482E-83FB-DB6C39C68AEA	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ReleaseEipAddress
&AllocationId=eip-2zeerraiwb7uj6i0d****
&<Common request parameters>
```

Sample success responses

XML format

```
<ReleaseEipAddressResponse>
  <RequestId>748C38F6-9A3D-482E-83FB-DB6C39C68AEA</RequestId>
</ReleaseEipAddressResponse>
```

JSON format

```
{
  "RequestId": "748C38F6-9A3D-482E-83FB-DB6C39C68AEA"
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidAllocationId.NotFound	Specified allocation ID is not found	The error message returned because the specified EIP does not exist. Check whether the value of the parameter is valid.
400	IncorrectEipStatus	Current elastic IP status does not support this operation.	The error message returned because the state of the EIP does not support this operation.
500	InternalServerError	The request processing has failed due to some unknown error.	The error message returned because an unknown error occurred.
404	Forbidden.RegionNotFound	Specified region is not found during access authentication.	The error message returned because the specified region does not exist. Check whether the specified region ID is valid.
400	Forbidden.ChargeTypesPrepaid	It's forbidden to release a prepaid EIP	The error message returned because you cannot release subscription EIPs.
400	Forbidden	The eip instance owner error	The error message returned because you are unauthorized to perform the operation on the EIP.
400	TaskConflict.AssociateGlobalAccelerationInstance	Operate too frequent.	The error message returned because the number of requests that you send exceeds the upper limit.

6.5.11. DescribeEipGatewayInfo

Queries information about the gateway and subnet mask of an elastic IP address (EIP).

Description

You can query only EIPs that are associated with secondary elastic network interfaces (ENIs) in multi-EIP to ENI mode.

Request parameters

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

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	eni-bp1d66qjxb3qoin3****	The ID of the secondary ENI that is associated with the EIP.
RegionId	String	Yes	cn-qingdao-env17-d01	The region to which the EIP that you want to query belongs. You can call the <code>DescribeRegions</code> operation to query region IDs.

Response parameters

Parameter	Type	Example	Description
Code	String	200	The status code of the operation.
EipInfos	Array of EipInfo		Detailed information about the EIP.
EipInfo			
Ip	String	47.XX.XX.236	The IP address of the EIP.
IpGw	String	47.XX.XX.1	The IP address of the gateway that is associated with the EIP.
IpMask	String	255.255.255.0	The subnet mask of the EIP.
Message	String	successful	The result of the operation.
RequestId	String	COFD0EED-F90D-4479-803D-DD62335357E5	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeEipGatewayInfo
&InstanceId=eni-bp1d66qjxb3qoin3****
&RegionId=cn-qingdao-env17-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeEipGatewayInfoResponse>
  <Message>successful</Message>
  <RequestId>C0FD0EED-F90D-4479-803D-DD62335357E5    </RequestId>
  <Code>200</Code>
  <EipInfos>
    <IpMask>255.255.255.0</IpMask>
    <IpGw>47.XX.XX.1</IpGw>
    <Ip>47.XX.XX.236</Ip>
  </EipInfos>
</DescribeEipGatewayInfoResponse>
```

JSON format

```
{
  "Message": "successful",
  "RequestId": "C0FD0EED-F90D-4479-803D-DD62335357E5",
  "Code": 200,
  "EipInfos": {
    "IpMask": "255.255.255.0",
    "IpGw": "47.XX.XX.1",
    "Ip": "47.XX.XX.236"
  }
}
```

Error codes

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. Apply for permissions and try again.

6.5.12. DescribeEipMonitorData

Queries the monitoring data of an elastic IP address (EIP).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEipMonitorData	The operation that you want to perform. Set the value to DescribeEipMonitorData .
AllocationId	String	Yes	eip-2zeerraiwb7uj6idcfv****	The ID of the EIP.

Parameter	Type	Required	Example	Description
EndTime	String	Yes	2017-01-05T01:05:10Z	The end of the time range to query. The time must be in UTC. The time follows the ISO 8601 standard and is displayed in the YYYY-MM-DDThh:mm:ssZ format. Example: 2013-01-10T12:00:00Z, which specifies 20:00:00 (UTC+8) on January 10, 2013. If the value of seconds (ss) is not 00, the end time is automatically rounded up to the next minute.
StartTime	String	Yes	2017-01-05T02:05:05Z	The beginning of the time range to query. The time must be in UTC. The time follows the ISO 8601 standard and is displayed in the YYYY-MM-DDThh:mm:ssZ format. Example: 2013-01-10T12:00:00Z, which specifies 20:00:00 (UTC+8) on January 10, 2013. If the value of seconds (ss) is not 00, the start time is automatically rounded up to the next minute.
RegionId	String	Yes	cn-hangzhou	The ID of the region to which the EIP belongs.
Period	Integer	No	60	The duration of each monitoring data entry. Valid values: 60, 300, 900, and 3600. Default value: 60. Unit: seconds. - If the value of (EndTime-StartTime)/Period is greater than 200, a maximum of 200 monitoring data entries are returned at a time. - If the value of (EndTime-StartTime)/Period is less than or equal to 200, only the monitoring data collected between the start time and end time are returned.

Response parameters

Parameter	Type	Example	Description
EipMonitorData	Array of EipMonitorData		The detailed information about the monitoring data of the EIP.
EipMonitorData			

Parameter	Type	Example	Description
EipBandwidth	Integer	10	The bandwidth. This value is equal to that of EipFlow/60. Unit: bit/s.
EipFlow	Integer	675	The sum of the inbound and outbound bandwidth.
EipPackets	Integer	3434	The number of packages.
EipRX	Long	122	The inbound bandwidth. Unit: Bit/s.
EipTX	Long	343	The outbound bandwidth. Unit: Bit/s.
TimeStamp	String	2010-01-21T09:50:23Z	The timestamp of the monitoring data. The time follows the ISO 8601 standard. Example: 2018-12-20T03:14:00Z.
RequestId	String	C8B26B44-0189-443E-9816-D951F59623A9	The ID of the request.

Examples

Sample requests

```
https://vpc.aliyuncs.com/?Action=DescribeEipMonitorData
&AllocationId=eip-2zeerraiwb7uj6idcfv****
&EndTime=2017-01-05T01:05:10Z
&StartTime=2017-01-05T02:05:05Z
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeEipMonitorDataResponse>
  <RequestId>B7D72D42-8A6C-4764-963B-5F7C049FA769</RequestId>
  <EipMonitorDatas>
    <EipMonitorData>
      <TimeStamp>2019-05-29T03:39:00Z</TimeStamp>
      <EipFlow>32666910</EipFlow>
      <EipTX>140370</EipTX>
      <EipPackets>23700</EipPackets>
      <EipRX>32526540</EipRX>
      <EipBandwidth>544448</EipBandwidth>
    </EipMonitorData>
    <EipMonitorData>
      <TimeStamp>2019-05-29T03:40:00Z</TimeStamp>
      <EipFlow>43020</EipFlow>
      <EipTX>17730</EipTX>
      <EipPackets>120</EipPackets>
      <EipRX>25290</EipRX>
      <EipBandwidth>717</EipBandwidth>
    </EipMonitorData>
  </EipMonitorDatas>
</DescribeEipMonitorDataResponse>
```

JSON **format**

```
{
  "DescribeEipMonitorDataResponse": {
    "RequestId": "B7D72D42-8A6C-4764-963B-5F7C049FA769",
    "EipMonitorDatas": {
      "EipMonitorData": [
        {
          "TimeStamp": "2019-05-29T03:39:00Z",
          "EipFlow": 32666910,
          "EipTX": 140370,
          "EipPackets": 23700,
          "EipRX": 32526540,
          "EipBandwidth": 544448
        },
        {
          "TimeStamp": "2019-05-29T03:40:00Z",
          "EipFlow": 43020,
          "EipTX": 17730,
          "EipPackets": 120,
          "EipRX": 25290,
          "EipBandwidth": 717
        }
      ]
    }
  }
}
```

Error codes

HttpCode	Error code	Error message	Description
404	InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	The error message returned because the specified Elastic Compute Service (ECS) instance is not found in the specified VPC.
400	InvalidStartTime.Malformed	The specified parameter "StartTime" is not valid.	The error message returned because the start time is invalid.
400	InvalidEndTime.Malformed	The specified parameter "EndTime" is not valid.	The error message returned because the end time is invalid.
400	InvalidPeriod.ValueNotSupported	The specified parameter "Period" is not valid.	The error message returned because the value of the Period parameter is invalid.
400	InvalidStartTime.TooEarly	The specified parameter "StartTime" is too early.	The error message returned because the start time is invalid.
400	InvalidAllocationId.NotFound	Specified allocation id is not found.	The error message returned because the specified EIP does not exist. Check whether the EIP is valid.
400	OperationDenied.TooManyDataQueried	Specified operation is denied as too many data to return.	The error message returned because an excessive amount of data is returned for a single query.
404	Forbidden.RegionNotFound	Specified region is not found during access authentication.	The error message returned because the specified region does not exist. Check whether the region ID is valid.

6.5.13. MoveResourceGroup

Moves a resource to a different resource group.

Request parameters

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

Parameter	Type	Required	Example	Description
NewResourceGroupId	String	Yes	rg-acfm3peow3k***	The ID of the resource group to which the cloud resource is to be moved.  Note You can use resource groups to manage resources owned by your Apsara Stack account. Resource groups simplify the resource and permission management of your Apsara Stack account.
RegionId	String	Yes	cn-qingdao-env17-d01	The region ID of the cloud resource. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
ResourceId	String	Yes	vpc-hp31psbg8ec3023s6****	The ID of the instance that you want to move.
ResourceType	String	Yes	vpc	The type of the cloud resource. Valid values: vpc: a virtual private cloud (VPC) eip: an elastic IP address (EIP)

Response parameters

Parameter	Type	Example	Description
RequestId	String	F84A05B3-7275-4C8B-8AEE-9088C639C271	The ID of the request.

Examples

Sample requests

```

http(s)://[Endpoint]/?Action=MoveResourceGroup
&NewResourceGroupId=rg-acfm3peow3k****
&RegionId=cn-qingdao-env17-d01
&ResourceId=vpc-hp31psbg8ec3023s6****
&ResourceType=vpc
&<Common request parameters>

```

Sample success responses

XML format

```
<MoveResourceGroup>
  <RequestId>F84A05B3-7275-4C8B-8AEE-9088C639C271</RequestId>
</MoveResourceGroup>
```

JSON format

```
{
  "RequestId": "F84A05B3-7275-4C8B-8AEE-9088C639C271"
}
```

Error codes

HttpCode	Error code	Error message	Description
400	InvalidResourceGroupId	The specified ResourceGroupId does not exist.	The error message returned because the specified resource group ID is invalid.

6.5.14.

DescribeHighDefinitionMonitorLogAttribute

Queries configurations about the fine-grained monitoring feature of an elastic IP address (EIP).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeHighDefinitionMonitorLogAttribute	The operation that you want to perform. Set the value to DescribeHighDefinitionMonitorLogAttribute .
InstanceId	String	Yes	eip-wz9fi6qbobo9fwgx7****	The ID of the instance whose fine-grained monitoring configurations you want to query.
RegionId	String	Yes	cn-qingdao-env66-d01	The region ID of the instance. You can call the <code>DescribeRegions</code> operation to query the most recent region list.
InstanceType	String	No	EIP	The type of the instance. Set the value to EIP .

Response parameters

Parameter	Type	Example	Description
InstanceId	String	eip-wz9fi6qboho9fwgx7****	The ID of the instance whose fine-grained monitoring configurations you want to query.
InstanceType	String	EIP	The type of the monitoring instance that is queried. The value is set to EIP .
LogProject	String	hdmonitor-cn-qingdao-165820696****	The name of the project of Log Service.
LogStore	String	hdmonitor	The name of the Logstore of Log Service.
RequestId	String	54B48E3D-DF70-471B-AA93-08E683A1B457	The ID of the request.
Success	String	true	Indicates whether the operation is performed. Valid values: true: yes false: no

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeHighDefinitionMonitorLogAttribute
&InstanceId=eip-wz9fi6qboho9fwgx7****
&RegionId=cn-qingdao-env66-d01
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeHighDefinitionMonitorLogAttribute>
  <RequestId>54B48E3D-DF70-471B-AA93-08E683A1B457</RequestId>
  <LogStore>hdmonitor</LogStore>
  <InstanceId>eip-wz9fi6qboho9fwgx7****</InstanceId>
  <InstanceType>EIP</InstanceType>
  <LogProject>hdmonitor-cn-qingdao-165820696****</LogProject>
  <Success>true</Success>
</DescribeHighDefinitionMonitorLogAttribute>
```

JSON format

```
{
  "DescribeHighDefinitionMonitorLogAttribute": {
    "RequestId": "54B48E3D-DF70-471B-AA93-08E683A1B457",
    "LogStore": "hdmonitor",
    "InstanceId": "eip-wz9fi6qboho9fwgx7****",
    "InstanceType": "EIP",
    "LogProject": "hdmonitor-cn-qingdao-165820696****",
    "Success": true
  }
}
```

7. Appendixes

7.1. Process of API calls by using the ASAPI gateway

You can use the Apsara Stack API (ASAPI) gateway to call API operations of most Apsara Stack services. This topic describes how to call an API operation of an Apsara Stack service by using the ASAPI gateway.

Procedure

1. Obtain Apsara Stack SDKs.

Before you use the ASAPI gateway to make an API call, you must obtain Apsara Stack SDKs. For more information, see [Obtain Apsara Stack SDKs](#).

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 the API call.

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 value of the RegionID parameter that is required for the API call.

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, 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 by default.
- 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.

6. View the developer guide of the cloud service that you want to use to learn how to make the API call.

View the developer guide of the cloud service that you want to use. This way, you can learn the features of API operations and how to call the API operations. For more information, see [Use developer guides](#).

7. Use Apsara Stack SDKs to make an API call.

After you complete the preceding steps, you can use Apsara Stack SDKs to make an API call. You can refer to API Reference for details about how to make the API call based on the programming language that you use.

In the following sample code, Java and the DescribeInstances API operation of Elastic Compute Service (ECS) are used. Sample code:

```
public static void main(String[] args) {
    ASClient client = new ASClient();
    // Specify the source of the call. This parameter is used only for logging.
    client.setSdkSource("autoTest");

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

    parameters.put("Product", "Ecs");// Specify the service code to be the same as the
    one displayed in the corresponding API directory.

    parameters.put("Action", "DescribeInstances");// Specify the name of the API opera-
    tion. The name must be case-sensitive and the same as that displayed in the API directo-
    ry.

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

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

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

    // Specify the following parameters for this API call. The parameters are case-sens-
    itive.
    parameters.put("PageNumber",1);
    parameters.put("PageSize",10);

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

    // Specify the obtained 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), Serializ-
    erFeature.PrettyFormat));
}
```

7.2. Use the ASAPI gateway to make API calls

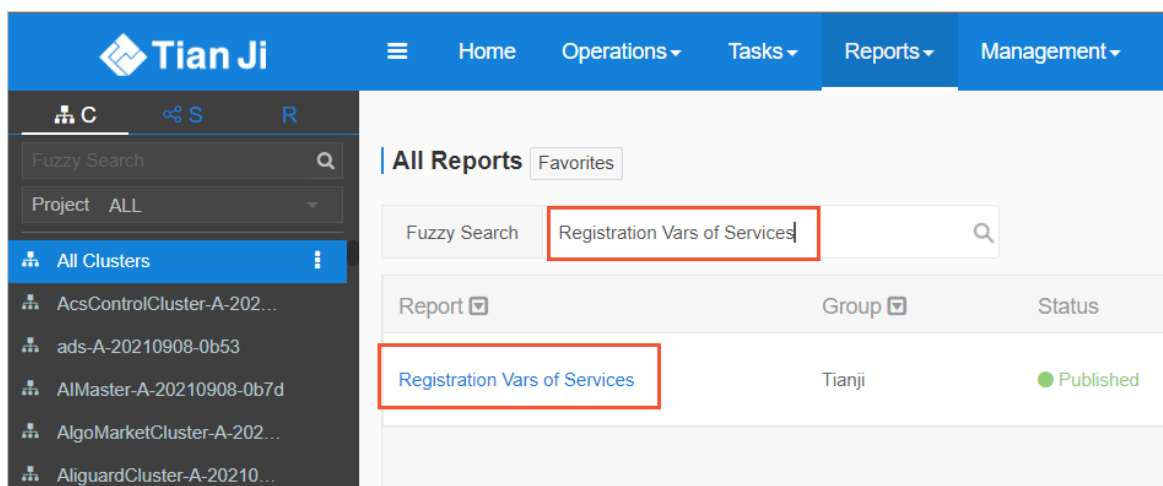
7.2.1. Obtain an endpoint of ASAPI

This topic describes three methods that you can use to obtain an endpoint of Apsara Stack API (ASAPI) and 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` and click the report name.



- On the **Registration Vars of Services** page, click the  icon next to **Service** and search for `asapi`.
- Find the `asapi` service, right-click 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`.
- Generate an endpoint of ASAPI based on 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.
 - Log on to the Apsara Uni-manager Operations Console.
 - In the top navigation bar, click **Products**.
 - Choose **Platforms > Apsara Infrastructure Management Framework**.

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

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

```
{
  "domain": "public.asapi.<region>.<internet-domain>.com",
  "ha_apply_type": "active-active",
  "name": "asapi_dns_public",
  "vip": "10.0.0.1"
}
```

4. Generate an endpoint of ASAPI based on the following format:

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

Method 3: Concatenate strings to generate an endpoint

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

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

Note

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

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

```
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 them with the actual values that you obtained.

Available endpoint example:

```
root@ ~ # curl https://public.asapi.us-east-1.amazonaws.com/api/version -k
{"version":"v3.13","code":"200","apiCount":12379,"desc":"update xml pretty"}root@ ~
```

Unavailable endpoint example:

```
[root@ ~]# curl https://public.asapi.us-east-1.amazonaws.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 in the following format:

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

Note

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

Procedure

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

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

Note

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

2. Enter your username and password.

Note

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

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

To enhance security, 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 is 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 Apsara Infrastructure Management.
 5. In the left-side navigation pane, choose **Operations > Cluster Operations**.
 6. On the **Clusters** page, enter **ascm-A** in the Cluster search box to find the cluster. Click the cluster name.
 7. On the **Cluster Dashboard** page, click **Operations Menu > Configuration Files**.
 8. In the **File List** window on the left side of the **Cluster Configuration** page, click **kv.conf**, click the file content in the right window, and then press Ctrl + F. Search for region, internet-domain, and intranet-domain.

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

 Note

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

7.2.2. Obtain the ASAPI SDK

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

Public environment

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

Private environment

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

ASAPI SDK for Java

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.

Parameter	Type	Required	Example	Description
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	<pre>{"Statement": [{"Action": ["*"], "Effect": "Allow", "Resource": ["*"]}], "Version": "1"}</pre>	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.

Parameter	Type	Example	Description
AccessKeyId	String	STS.L4aBSCSJVMuKg5U1****	The AccessKey ID.
AccessKeySecret	String	wyLT SmsyPGP1ohvw8xYgB29dIGi8KMiH2pK****	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.alivuncs.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.aliyuncs.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.aliyuncs.com");
        request.setSysProduct("Sts");
        request.setSysAction("AssumeRole");
        request.setSysVersion("2015-04-01");
        request.setSysMethod(MethodType.POST);
        request.setHttpContentType(FormatType.FORM);
        // Replace "<yourRoleSessionName>" with the alias that you specify for the current role session.
        request.putQueryParameter("RoleSessionName", "<yourRoleSessionName>");
        // Replace "<yourRoleArn>" with the actual ARN that you obtained for the RAM role in the preceding step.
        request.putQueryParameter("RoleArn", "<yourRoleArn>");
        try {
            CommonResponse response = client.getCommonResponse(request);
            String assumeRole = response.getData();
            if (StringUtils.isEmpty(assumeRole)) return;
            JSONObject assumeRoleJson = JSONObject.parseObject(assumeRole);
            JSONObject credentials = assumeRoleJson.getJSONObject("Credentials");
            // Obtain the STS AccessKey 3-tuple.
            String stsAK = credentials.getString("AccessKeyId");
            String stsSK = credentials.getString("AccessKeySecret");
            String stsToken = credentials.getString("SecurityToken");
            System.out.println("stsAk: " + stsAK + "\nstsSk: " + stsSK + "\nstsToken: " + stsToken);
        } catch (ServerException e) {
            System.out.println(e.getErrCode());
            System.out.println(e.getErrMsg());
        } catch (ClientException e) {
            System.out.println(e.getErrCode());
        }
    }
}

```

```

        System.out.println(e.getErrMsg());
    }
}
}

```

Call examples

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

```

package com.aliyuns.test;

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

public class DescribeZonesDemo {
    public static void main(String[] args) {
        // Replace "<yourRegionID>" with the actual region ID.
        // Replace "<yourStsAccesskey>" and "<yourStsAccessKeySecret>" with the AccessKey ID and secret in the 3-tuple that you obtained in the 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.aliyuns.com");
        request.setSysProduct("Ecs");
        request.setSysAction("DescribeZones");
        request.setSysVersion("2014-05-26");
        request.setSysMethod(MethodType.POST);
        request.setHttpContentType(FormatType.FORM);
        //Replace "<yourRegionID>" with the actual region ID.
        request.putHeadParameter("x-acs-regionid", "<yourRegionID>");
        // Replace "<yourStsToken>" with the STS token in the 3-tuple that you obtained in the preceding step.
        request.putQueryParameter("SecurityToken", "<yourStsToken>");
        // Optional. Specify the resource set ID.
        // request.putHeadParameter("x-acs-resourcegroupid", "<yourResourceGroupID>");
        // Required. Specify the organization ID.
        request.putHeadParameter("x-acs-organizationid", "<yourOrganizationID>");
        try {
            CommonResponse response = client.getCommonResponse(request);

```

```

        System.out.println(response.getData());
    } catch (ServerException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    } catch (ClientException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    }
}
}
}

```

Error codes

HttpCode	Error code	Error message	Description
400	InvalidParameter	The parameter RoleArn is wrongly formed.	The error message returned because the ARN format of the RAM role is invalid.
400	InvalidParameter.RoleArn	The parameter RoleArn is wrongly formed.	The error message returned because the ARN format of the RAM role is invalid.
400	InvalidParameter.RoleSessionName	The parameter RoleSessionName is wrongly formed.	The error message returned because the value of the RoleSessionName parameter is in an invalid format. The value must be 2 to 64 characters in length and can contain letters, digits, periods (.), at signs (@), hyphens (-), and underscores (_).

HttpCode	Error code	Error message	Description
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.
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.