Virtual Private Cloud

API Reference

Issue 01

Date 2024-07-31

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Before You Start

1.1 Overview

Welcome to *Virtual Private Cloud API Reference*. The Virtual Private Cloud (VPC) service enables you to provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs), improving the security of resources in the cloud system and simplifying network deployment.

This document describes how to use application programming interfaces (APIs) to perform operations on VPCs, such as creating, querying, deleting, and updating a VPC. For details about all supported operations, see **API Overview**.

If you plan to access VPCs through an API, ensure that you are familiar with VPC concepts. For details, see **Service Overview** in *Virtual Private Cloud User Guide*.

1.2 API Calling

VPC supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details about API calling, see **Calling APIs**.

Additionally, VPCs offer software development kits (SDKs) for multiple programming languages. For details about how to use SDKs, log in at **HUAWEI CLOUD SDKs**.

1.3 Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

1.4 Notes and Constraints

The number of VPCs that you can create is determined by your quota. To view or increase the quota, see **What Is a Quota?**

For more constraints, see API description.

1.5 Concepts

- Account

  An account is created upon successful signing up. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity, which should not be used directly to perform routine management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

- User

  An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  API authentication requires information such as the account name, username, and password.

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

  For details, see **Region and AZ**.

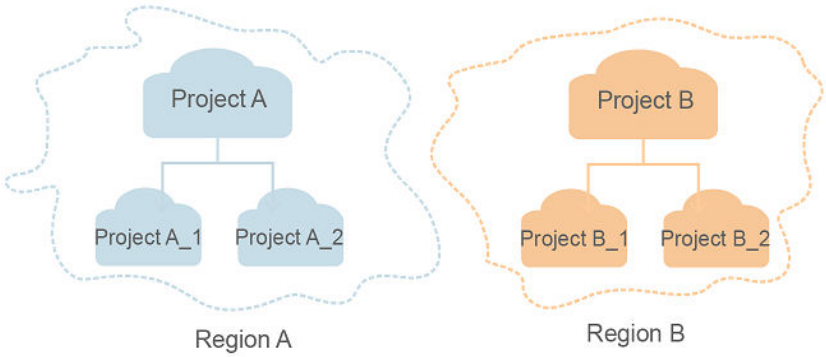
- AZ

  An AZ comprises of one or more physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Computing, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

- Project

  A project corresponds to a region. Default projects are defined to group and physically isolate resources (including computing, storage, and network resources) across regions. Users can be granted permissions in a default project to access all resources under their accounts in the region associated with the project. If you need more refined access control, create subprojects under a default project and create resources in subprojects. Then you can assign users the permissions required to access only the resources in the specific subprojects.

Figure 1-1 Project isolation model



- Enterprise Project

  Enterprise projects group and manage resources across regions. Resources in different enterprise projects are logically isolated. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects.

  For details about enterprise projects and about how to obtain enterprise project IDs, see ***Enterprise Management User Guide***.

1.6 Selecting an API Type

The following APIs have been abandoned and are not recommended:

- **Creating a Port (Discarded)**
- **Querying a Port (Discarded)**
- **Querying Ports (Discarded)**
- **Updating a Port (Discarded)**
- **Deleting a Port (Discarded)**

2 API Overview

VPC APIs include both native OpenStack APIs and extension APIs.

A combination of these two types of APIs allows you to use all functions provided by the VPC service. If a function involves both native OpenStack APIs and extension VPC APIs, use extension VPC APIs preferentially.

VPC APIs

Table 2-1 API description

Type	Description
Virtual Private Cloud	APIs for creating, querying, updating, and deleting VPCs
Subnet	APIs for creating, querying, updating, and deleting subnets
Quota	API for querying quota values
Private IP Address	APIs for assigning, querying, and releasing private IP addresses
Security Group	• APIs for creating, querying, and deleting security groups • APIs for creating, querying, and deleting security group rules
Port	APIs for creating, querying, updating, and deleting ports
VPC Peering Connection	• APIs for creating, querying, updating, and deleting VPC peering connections • APIs for accepting and rejecting VPC peering connection requests
VPC Route	APIs for creating, querying, and deleting VPC routes
VPC Tag Management	• APIs for adding tags to VPCs, as well as querying and deleting VPC tags • APIs for adding tags to subnets as well as querying and deleting subnet tags

Type	Description
VPC Flow Log	APIs for creating, querying, updating, and deleting VPC flow logs This type of APIs is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, LA-Mexico City2, and AF-Johannesburg.

VPC v3 APIs

Table 2-2 API description

Type	Description
VPC v3	• APIs for querying and editing secondary CIDR blocks. • This type of APIs is now available in CN North-Beijing1, CN North-Beijing2, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, TR-Istanbul, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.
Security Groups	• APIs for creating, querying, updating, and deleting security groups. • This type of APIs is now available in CN North-Beijing1, CN North-Beijing2, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, TR-Istanbul, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.
Security Group Rule	• APIs for creating, querying, and deleting security group rules. • This type of APIs is now available in CN North-Beijing1, CN North-Beijing2, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, TR-Istanbul, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.

Type	Description
IP Address Group	• APIs for creating, querying, updating, and deleting IP address groups. • This type of APIs is now available in CN North-Beijing1, CN North-Beijing2, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, TR-Istanbul, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.
Supplementary Network Interface	• APIs for creating, querying, updating, and deleting supplementary network interfaces. • This type of APIs is now available in CN North-Beijing4, CN North-Beijing2, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Singapore, AP-Jakarta, LA-Mexico City2, and TR-Istanbul.
Network ACL	• APIs for creating, querying, updating, and deleting network ACLs. • This type of APIs is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.
Ports	• APIs for adding a port to or removing a port from a security group. • This type of APIs is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, AP-Bangkok, and CN-Hong Kong.

Native OpenStack APIs

Table 2-3 Native OpenStack APIs

Type	Description
API Version Information	APIs for querying all available API versions and displaying the results in pages.
Port	APIs for creating, querying, updating, and deleting ports
Network	APIs for creating, querying, updating, and deleting networks
Subnet	APIs for creating, querying, updating, and deleting subnets
Router	APIs for creating, querying, updating, and deleting routers

Type	Description
Network ACL	• APIs for creating, updating, and releasing network ACLs • APIs for creating, updating, deleting, and querying network ACL rules. • APIs for creating, updating, deleting, and querying network ACL policies
Security Group	• APIs for creating, querying, updating, and deleting security groups • APIs for creating, querying, and deleting security group rules

3 Calling APIs

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for **creating an IAM User** as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

{URI-scheme}://{Endpoint}/{resource-path}?{query-string}

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

Table 3-1 URI parameter description

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**. For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
resource-path	Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.

Parameter	Description
query-string	Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of *Parameter name*=*Parameter value*. For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

IAM is a global service. You can create an IAM user using the endpoint of IAM in any region. For example, to create an IAM user in the **CN-Hong Kong** region, obtain the endpoint of IAM (**iam.ap-southeast-1.myhuaweicloud.com**) for this region and the **resource-path** (**/v3.0/OS-USER/users**) in the URI of the API for **creating an IAM user**. Then construct the URI as follows:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
```

Figure 3-1 Example URI

NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server.

Table 3-2 HTTP methods

Method	Description
GET	Requests the server to return specified resources.
PUT	Requests the server to update specified resources.
POST	Requests the server to add resources or perform special operations.
DELETE	Requests the server to delete specified resources, for example, an object.
HEAD	Same as GET except that the server must return only the response header.

Method	Description
PATCH	Requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API for **creating an IAM user**, the request method is **POST**. An example request is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows.

Table 3-3 Common request header fields

Parameter	Description	Mandatory	Example Value
Host	Specifies the server domain name and port number of the resources being requested. The value can be obtained from the URL of the service API. The value is in the format of *Hostname:Port number*. If the port number is not specified, the default port is used. The default port number for **https** is **443**.	No This field is mandatory for AK/SK authentication.	code.test.com or code.test.com:443
Content-Type	Specifies the type (or format) of the message body. The default value **application/json** is recommended. Other values of this field will be provided for specific APIs if any.	Yes	application/json
Content-Length	Specifies the length of the request body. The unit is byte.	No	3495

Parameter	Description	Mandatory	Example Value
X-Project-Id	Specifies the project ID. Obtain the project ID by following the instructions in **Obtaining a Project ID**.	No This field is mandatory for requests that use AK/SK authentication in the Dedicated Cloud (DeC) scenario or multi-project scenario.	e9993fc787d94b6c886cbaa340f9c0f4
X-Auth-Token	Specifies the user token. It is a response to the API for **obtaining a user token** (This is the only API that does not require authentication). After the request is processed, the value of **X-Subject-Token** in the response header is the token value.	No This field is mandatory for token authentication.	The following is part of an example token: MIIPAgYJKoZIhvcNAQcCo...ggg1BBIINPXsidG9rZ

NOTE

In addition to supporting authentication using tokens, APIs support authentication using AK/SK, which uses SDKs to sign a request. During the signature, the **Authorization** (signature authentication) and **X-Sdk-Date** (time when a request is sent) headers are automatically added in the request.

For more details, see "Authentication Using AK/SK" in **Authentication**.

The following shows an example request of the API for **creating an IAM user** when AK/SK authentication is used:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date, Signature=**********
```

(Optional) Request Body

This part is optional. A request body is generally sent in a structured format (for example, JSON or XML), which is specified by **Content-Type** in the request header. It is used to transfer content other than the request header. If the request body contains full-width characters, these characters must be coded in UTF-8.

The request body varies depending on APIs. Certain APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

The following shows an example request (a request body included) of the API for **creating an IAM user**. You can learn about request parameters and related

description from this example. The bold parameters need to be replaced for a real request.

- **accountid**: account ID of an IAM user
- **username**: name of an IAM user
- **email**: email of an IAM user
- **password**: login password of an IAM user

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=**********, SignedHeaders=content-type;host;x-sdk-date,
Signature=**********

{
    "user": {
        "domain_id": "accountid",
        "name": "username",
        "password": "**********",
        "email": "email",
        "description": "IAM User Description"
    }
}
```

If all data required for the API request is available, you can send the request to call the API through **curl**, **Postman**, or coding. In the response to the API used to obtain a user token, **X-Subject-Token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token authentication: Requests are authenticated using tokens.
- AK/SK authentication: Requests are encrypted using AK/SK pairs. AK/SK authentication is recommended because it is more secure than token authentication.

Token Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API. You can obtain a token by calling the **Obtaining User Token** API.

VPC is a project-level service. When you call the API, set **auth.scope** in the request body to **project**.

```
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
```



```
        "password": {
          "user": {
            "name": "username",   // IAM user name
            "password": "********",  // IAM user password
            "domain": {
              "name": "domainname"  // Name of an IAM account
            }
          }
        }
      },
      "scope": {
        "project": {
          "name": "xxxxxxxx"    // Project name
        }
      }
    }
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK Authentication

NOTE

AK/SK authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token authentication is recommended.

In AK/SK authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key, which is used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK authentication, you can use an AK/SK to sign requests based on the signature algorithm or using the signing SDK. For details about how to sign requests and use the signing SDK, see **API Request Signing Guide**.

NOTE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

3.3 Response

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see **Status Codes**.

For example, if status code **201** is returned for calling the API used to **create an IAM user**, the request is successful.

Response Header

Similar to a request, a response also has a header, for example, **Content-Type**.

Figure 3-2 shows the response header fields for the API used to **create an IAM user**. The **X-Subject-Token** header field is the desired user token. This token can then be used to authenticate the calling of other APIs.

NOTE

For security purposes, you are advised to set the token in ciphertext in configuration files or environment variables and decrypt it when using it.

Figure 3-2 Header fields of the response to the request for creating an IAM user

```
"X-Frame-Options": "SAMEORIGIN",
"X-IAM-ETag-id": "2562365939-d8f6f12921974cb097338ac11fceac8a",
"Transfer-Encoding": "chunked",
"Strict-Transport-Security": "max-age=31536000; includeSubdomains;",
"Server": "api-gateway",
"X-Request-Id": "af2953f2bcc67a42325a69a19e6c32a2",
"X-Content-Type-Options": "nosniff",
"Connection": "keep-alive",
"X-Download-Options": "noopen",
"X-XSS-Protection": "1; mode=block;",
"X-IAM-Trace-Id": "token_[redacted]_null_af2953f2bcc67a42325a69a19e6c32a2",
"Date": "Tue, 21 May 2024 09:03:40 GMT",
"Content-Type": "application/json; charset=utf8"
```

(Optional) Response Body

The body of a response is often returned in a structured format (for example, JSON or XML) as specified in the **Content-Type** header field. The response body transfers content except the response header.

The following is part of the response body for the API used to **create an IAM user**.

```
{
    "user": {
        "id": "c131886aec...",
        "name": "IAMUser",
        "description": "IAM User Description",
        "areacode": "",
        "phone": "",
        "email": "***@***.com",
        "status": null,
        "enabled": true,
        "pwd_status": false,
        "access_mode": "default",
        "is_domain_owner": false,
        "xuser_id": "",
        "xuser_type": "",
        "password_expires_at": null,
        "create_time": "2024-05-21T09:03:41.000000",
        "domain_id": "d78cbac1.....",
        "xdomain_id": "30086000.....",
        "xdomain_type": "",
        "default_project_id": null
```



```
    }
}
```

If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

```
{
    "error_msg": "The request message format is invalid.",
    "error_code": "IMG.0001"
}
```

In the response body, **error_code** is an error code, and **error_msg** provides information about the error.

4 APIs

4.1 Virtual Private Cloud

4.1.1 Creating a VPC

Function

This API is used to create a VPC.

URI

POST /v1/{project_id}/vpcs

Table 4-1 describes the parameters.

Table 4-1 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-2 Request parameter

Parameter	Mandatory	Type	Description
vpc	Yes	**vpc** object	**Specifies the VPC objects.**

Table 4-3 VPC objects

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the VPC name. • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). • Each VPC name of a tenant must be unique if the VPC name is not left blank.
description	No	String	• Provides supplementary information about the VPC. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	No	String	• Specifies the available IP address ranges for subnets in the VPC. • Possible values are as follows: – 10.0.0.0/8-24 – 172.16.0.0/12-24 – 192.168.0.0/16-24 • If **cidr** is not specified, the default value is left blank. • The value must be in CIDR format, for example, **192.168.0.0/16**.
enterprise_project_id	No	String	• Specifies the enterprise project ID. When creating a VPC, you can associate an enterprise project ID with the VPC. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.

Parameter	Mandatory	Type	Description
tags	No	Array of Strings	• Specifies VPC tags. When creating a VPC, you can add tags to the VPC. • Each VPC can have up to 10 tags. – **key**: Tag key. The key cannot be empty and can contain up to 128 characters (36 characters on the console). It can consist of letters, digits, underscores (_), and hyphens (-). Tag keys of a resource must be unique. – **value**: Tag value. The value can contain up to 255 characters (43 characters on the console). It can consist of letters, digits, underscores (_), periods (.), and hyphens (-). • Format: [key*value]. The key and value of each tag are connected by an asterisk (*).

Example Request

- Create a VPC named **vpc** and set its CIDR block to 192.168.0.0/16.

```
POST https://{Endpoint}/v1/{project_id}/vpcs

{
    "vpc": {
        "name": "vpc",
        "description": "test",
        "cidr": "192.168.0.0/16",
        "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
    }
}
```

Response Parameters

Table 4-4 Response parameter

Parameter	Type	Description
vpc	**vpc** object	**Specifies the VPC objects.**

Table 4-5 VPC objects

Parameter	Type	Description
id	String	Specifies a resource ID in UUID format.

Parameter	Type	Description
name	String	• Specifies the VPC name. • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). • Each VPC name of a tenant must be unique if the VPC name is not left blank.
description	String	• Provides supplementary information about the VPC. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	• Specifies the available IP address ranges for subnets in the VPC. • Possible values are as follows: – 10.0.0.0/8-24 – 172.16.0.0/12-24 – 192.168.0.0/16-24 • If **cidr** is not specified, the default value is left blank. • The value must be in CIDR format, for example, **192.168.0.0/16**.
status	String	• Specifies the VPC status. • Possible values are as follows: – **CREATING**: The VPC is being created. – **OK**: The VPC is created successfully.
routes	Array of **route** objects	• Specifies the route information. • For details, see the description of the **route objects**.
enterprise_project_id	String	• Specifies the enterprise project ID. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.
tenant_id	String	• Project ID
created_at	String	• Specifies the time (UTC) when the VPC is created. • Format: *yyyy-MM-ddTHH:mm:ss*

Parameter	Type	Description
updated_at	String	• Specifies the time (UTC) when the VPC is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-6 route objects

Parameter	Type	Description
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in the CIDR format. IPv4 and IPv6 CIDR formats are supported.
nexthop	String	• Specifies the next hop of a route. • The value must be an IP address from the subnet of the VPC. IPv4 and IPv6 addresses are supported.

Example Response

```
{
 "vpc":
    {
    "id": "99d9d709-8478-4b46-9f3f-2206b1023fd3",
    "name": "vpc",
    "description": "test",
    "cidr": "192.168.0.0/16",
    "status": "CREATING",
    "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
    "routes": [],
    "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
    "created_at": "2022-12-15T02:25:11",
    "updated_at": "2022-12-15T02:25:11"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.1.2 Querying VPC Details

Function

This API is used to query details about a VPC.

URI

GET /v1/{project_id}/vpcs/{vpc_id}

Table 4-7 describes the parameters.

Table 4-7 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID, which uniquely identifies the VPC.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/vpcs/99d9d709-8478-4b46-9f3f-2206b1023fd3
```

Response Parameters

Table 4-8 Response parameter

Parameter	Type	Description
vpc	**vpc** object	**Specifies the VPC objects.**

Table 4-9 VPC objects

Parameter	Type	Description
id	String	Specifies a resource ID in UUID format.
name	String	• Specifies the VPC name. • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). • Each VPC name of a tenant must be unique if the VPC name is not left blank.

Parameter	Type	Description
description	String	• Provides supplementary information about the VPC. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	• Specifies the available IP address ranges for subnets in the VPC. • Possible values are as follows: – 10.0.0.0/8-24 – 172.16.0.0/12-24 – 192.168.0.0/16-24 • If **cidr** is not specified, the default value is left blank. • The value must be in CIDR format, for example, **192.168.0.0/16**.
status	String	• Specifies the VPC status. • Possible values are as follows: – **CREATING**: The VPC is being created. – **OK**: The VPC is created successfully.
routes	Array of **route** objects	• Specifies the route information. • For details, see the description of the **route objects**.
enterprise_project_id	String	• Enterprise project ID • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.
tenant_id	String	• Project ID
created_at	String	• Time (UTC) when the VPC is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the VPC is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-10 route objects

Parameter	Type	Description
destination	String	• Specifies the destination network segment of a route. • Constraints: The value must be in the CIDR format. IPv4 and IPv6 CIDR formats are supported.
nexthop	String	• Specifies the next hop of a route. • The value must be an IP address from the subnet of the VPC. IPv4 and IPv6 addresses are supported.

Example Response

```
{
    "vpc": {
        "id": "99d9d709-8478-4b46-9f3f-2206b1023fd3",
        "name": "vpc",
        "description": "test",
        "cidr": "192.168.0.0/16",
        "status": "OK",
        "enterprise_project_id": "0" ,
        "routes": [],
        "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
        "created_at": "2022-12-15T02:25:11",
        "updated_at": "2022-12-15T02:25:11"
}
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.1.3 Querying VPCs

Function

This API is used to query VPCs using search criteria and to display the VPCs in a list.

URI

GET /v1/{project_id}/vpcs

Example:

```
GET https://{Endpoint}/v1/{project_id}/vpcs?limit=10&marker=13551d6b-755d-4757-b956-536f674975c0
```

Table 4-11 describes the parameters.

Table 4-11 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
id	No	String	Specifies the VPC ID that is used as the filtering condition.
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	• Specifies the enterprise project ID that is used to filter out the VPCs associated with a specified enterprise project. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. To obtain the VPCs bound to all enterprise projects of the user, set **all_granted_eps**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/vpcs
```

Response Parameters

Table 4-12 Response parameter

Parameter	Type	Description
vpcs	Array of **vpc** objects	Specifies the **VPC objects**.

Table 4-13 VPC objects

Parameter	Type	Description
id	String	Specifies a resource ID in UUID format.
name	String	• Specifies the VPC name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). • Each VPC name of a tenant must be unique if the VPC name is not left blank.

Parameter	Type	Description
description	String	• Provides supplementary information about the VPC. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	• Specifies the available IP address ranges for subnets in the VPC. • Possible values are as follows: – 10.0.0.0/8-24 – 172.16.0.0/12-24 – 192.168.0.0/16-24 • If **cidr** is not specified, the value is left blank by default. • If **cidr** is specified, the value must be in CIDR format, for example, **192.168.0.0/16**.
status	String	• Specifies the VPC status. • Possible values are as follows: – **CREATING**: The VPC is being created. – **OK**: The VPC is created.
enterprise_project_id	String	• Specifies the enterprise project ID. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.
routes	Array of **route** objects	• Specifies the route information. • For details, see **Table 4-14**.
tenant_id	String	• Project ID
created_at	String	• Specifies the time (UTC) when the VPC is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the VPC is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-14 route objects

Parameter	Type	Description
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in the CIDR format. IPv4 and IPv6 CIDR formats are supported.
nexthop	String	• Specifies the next hop of a route. • The value must be an IP address from the subnet of the VPC. IPv4 and IPv6 addresses are supported.

Example Response


```
{
  "vpcs": [
    {
      "id": "13551d6b-755d-4757-b956-536f674975c0",
      "name": "default",
      "description": "test",
      "cidr": "172.16.0.0/16",
      "status": "OK",
      "enterprise_project_id": "0",
      "routes": [],
      "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
      "created_at": "2022-12-15T02:11:13",
      "updated_at": "2022-12-15T02:11:13"
    },
    {
      "id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
      "name": "222",
      "description": "test",
      "cidr": "192.168.0.0/16",
      "status": "OK",
      "enterprise_project_id": "0635d733-c12d-4308-ba5a-4dc27ec21038",
      "routes": [],
      "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
      "created_at": "2022-12-15T04:01:21",
      "updated_at": "2022-12-15T04:01:21"
    },
    {
      "id": "99d9d709-8478-4b46-9f3f-2206b1023fd3",
      "name": "vpc",
      "description": "test",
      "cidr": "192.168.0.0/16",
      "status": "OK",
      "enterprise_project_id": "0",
      "routes": [],
      "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
      "created_at": "2022-12-15T05:36:29",
      "updated_at": "2022-12-15T05:36:29"
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.1.4 Updating a VPC

Function

This API is used to update information about a VPC.

URI

PUT /v1/{project_id}/vpcs/{vpc_id}

Table 4-15 describes the parameters.

Table 4-15 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID, which uniquely identifies the VPC.

Request Parameters

Table 4-16 Request parameter

Parameter	Mandatory	Type	Description
vpc	Yes	**vpc** object	**Specifies the VPC objects.**

Table 4-17 VPC objects

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the VPC name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.). • Each VPC name of a tenant must be unique if the VPC name is not left blank.
description	No	String	• Provides supplementary information about the VPC. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	No	String	• Specifies the available IP address ranges for subnets in the VPC. • Possible values are as follows: – 10.0.0.0/8-24 – 172.16.0.0/12-24 – 192.168.0.0/16-24 • If **cidr** is not specified, the value is left blank by default. • Constraints: – The value must be in CIDR format, for example, **192.168.0.0/16**. – If you want to update the CIDR block of the VPC, the new CIDR block must contain all subnets in the VPC.
routes	No	Array of **route** objects	• Specifies the route list. For details, see **Table 4-18**.

Table 4-18 route objects

Parameter	Mandatory	Type	Description
destination	No	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in the CIDR format. IPv4 and IPv6 CIDR formats are supported.
nexthop	No	String	• Specifies the next hop of a route. • The value must be an IP address from the subnet of the VPC. IPv4 and IPv6 addresses are supported.

Example Request

- Change the name, description, and CIDR block of the VPC whose ID is 99d9d709-8478-4b46-9f3f-2206b1023fd3 to **vpc1**, **test1**, and **192.168.0.0/16**, respectively.

```
PUT https://{Endpoint}/v1/{project_id}/vpcs/99d9d709-8478-4b46-9f3f-2206b1023fd3

{
    "vpc": {
        "name": "vpc1",
        "description": "test1",
        "cidr": "192.168.0.0/16"
    }
}
```

Response Parameters

Table 4-19 Response parameter

Parameter	Type	Description
vpc	**vpc** object	**Specifies the VPC objects.**

Table 4-20 VPC objects

Parameter	Type	Description
id	String	Specifies a resource ID in UUID format.
name	String	Specifies the VPC name.
description	String	• Provides supplementary information about the VPC. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
cidr	String	• Specifies the available IP address ranges for subnets in the VPC. • Possible values are as follows: – 10.0.0.0/8-24 – 172.16.0.0/12-24 – 192.168.0.0/16-24 • If **cidr** is not specified, the default value is left blank. • The value must be in CIDR format, for example, **192.168.0.0/16**.
status	String	• Specifies the VPC status. • Possible values are as follows: – **CREATING**: The VPC is being created. – **OK**: The VPC is created successfully.
enterprise_project_id	String	• Specifies the enterprise project ID. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.
routes	Array of **route** objects	• Specifies the route information. • For details, see the description of the **route objects**.
tenant_id	String	• Project ID
created_at	String	• Specifies the time (UTC) when the VPC is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the VPC is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-21 route objects

Parameter	Type	Description
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in the CIDR format. IPv4 and IPv6 CIDR formats are supported.
nexthop	String	• Specifies the next hop of a route. • The value must be an IP address from the subnet of the VPC. IPv4 and IPv6 addresses are supported.

Example Response

```
{
    "vpc": {
        "id": "99d9d709-8478-4b46-9f3f-2206b1023fd3",
        "name": "vpc1",
        "description": "test1",
        "cidr": "192.168.0.0/16",
        "status": "OK",
        "enterprise_project_id": "0",
        "routes": [],
        "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
        "created_at": "2022-12-15T02:25:11",
        "updated_at": "2022-12-15T06:23:15"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.1.5 Deleting a VPC

Function

This API is used to delete a VPC.

URI

DELETE /v1/{project_id}/vpcs/{vpc_id}

Table 4-22 describes the parameters.

Table 4-22 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID that uniquely identifies the VPC.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/{project_id}/vpcs/13551d6b-755d-4757-b956-536f674975c0
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.2 Subnet

4.2.1 Creating a Subnet

Function

This API is used to create a subnet.

URI

POST /v1/{project_id}/subnets

Table 4-23 describes the parameters.

Table 4-23 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-24 Request parameter

Parameter	Mandatory	Type	Description
subnet	Yes	**subnet** object	Specifies the **subnet objects**.

Table 4-25 subnet objects

Parameter	Mandatory	Type	Description
name	Yes	String	• Specifies the subnet name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	• Provides supplementary information about the subnet. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	Yes	String	• Specifies the subnet CIDR block. • The value must be within the VPC CIDR block. • The value must be in CIDR format. The subnet mask cannot be greater than 28.
gateway_ip	Yes	String	• Specifies the gateway of the subnet. • The value must be an IP address in the subnet. • The value must be a valid IP address.

Parameter	Mandatory	Type	Description
ipv6_enable	No	Boolean	• Specifies whether IPv6 is enabled. • The value can be **true** (enabled) or **false** (disabled). • If this parameter is left blank, the system automatically sets it to **false** by default.
dhcp_enable	No	Boolean	• Specifies whether DHCP is enabled for the subnet. • The value can be **true** (enabled) or **false** (disabled). • If this parameter is left blank, the value is set to **true** by default. If this parameter is set to **false**, newly created ECSs cannot obtain IP addresses, and usernames and passwords cannot be injected using Cloud-init.
primary_dns	No	String	• Specifies the primary IP address of DNS server on the subnet. • The value must be an IP address. If the value is not specified, the default value will be left blank. For instructions about how to obtain a private DNS server address, see **What Are the Private DNS Server Addresses Provided by the DNS Service?** For instructions about how to DNS server address, see **Querying Name Servers**.

Parameter	Mandatory	Type	Description
secondary_dns	No	String	• Specifies the standby IP address of DNS server on the subnet. • The value must be an IP address. If the value is not specified, the default value will be left blank. If only **secondary_dns** is specified and **primary_dns** is not specified, **primary_dns** will automatically use the value of **secondary_dns**. If there is only one DNS server address, only **primary_dns** is displayed. For instructions about how to obtain a private DNS server address, see **What Are the Private DNS Server Addresses Provided by the DNS Service?** For instructions about how to DNS server address, see **Querying Name Servers**.
dnsList	No	Array of strings	• Specifies the DNS server address list of a subnet. This field is required if you need to use more than two DNS servers. • This parameter value is the superset of both DNS server address 1 and DNS server address 2. If the value is not specified, the default value will be left blank. For instructions about how to obtain a private DNS server address, see **What Are the Private DNS Server Addresses Provided by the DNS Service?** For instructions about how to DNS server address, see **Querying Name Servers**.
availability_zone	No	String	• Specifies the AZ to which the subnet belongs, which can be obtained from endpoints. For details, see **Endpoints**. • The value must be an existing AZ in the system. If the value is not specified, the default value will be left blank.

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	Specifies the ID of the VPC to which the subnet belongs.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the NTP server address or DHCP lease time configured for the subnet. For details, see **Table 4-26**.
tags	No	Array of Strings	• Specifies subnet tags. When creating a subnet, you can add tags to the subnet. • Each subnet can have up to 10 tags. – **key**: Tag key. The key cannot be empty and can contain up to 128 characters (36 characters on the console). It can consist of letters, digits, underscores (_), and hyphens (-). Tag keys of a resource must be unique. – **value**: Tag value. The value can contain up to 255 characters (43 characters on the console). It can consist of letters, digits, underscores (_), periods (.), and hyphens (-). • Format: [key*value]. The key and value of each tag are connected by an asterisk (*).

Table 4-26 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	• Specifies the NTP server address or DHCP lease expiration time configured for the subnet. • Constraints: The option **ntp** for **opt_name** indicates the NTP server configured for the subnet. Currently, only IPv4 addresses are supported. A maximum of four IP addresses can be configured, and each address must be unique. Multiple IP addresses must be separated using commas (,). The option **null** for **opt_name** indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. The option **addresstime** for **opt_name** indicates the DHCP lease expiration time of the subnet. The value can be **-1**, which indicates unlimited lease time, or *Number*+**h**. The number ranges from 1 to 30,000. For example, the value can be **5h**. The default value is **24h**.
opt_name	Yes	String	• Specifies the NTP server address or DHCP lease time configured for the subnet. • Currently, the value can only be set to **ntp** or **addresstime**.

Example Request

- Create a subnet with name set to **subnet**, CIDR block set to 192.168.20.0/24, and gateway IP address set to 192.168.20.1 in the VPC with ID of 3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85.

```
POST https://{Endpoint}/v1/{project_id}/subnets

{
    "subnet": {
        "name": "subnet",
        "description": "",
        "cidr": "192.168.20.0/24",
        "gateway_ip": "192.168.20.1",
```



```
        "ipv6_enable": true,
        "dhcp_enable": true,
        "primary_dns": "114.xx.xx.114",
        "secondary_dns": "114.xx.xx.115",
        "dnsList": [
            "114.xx.xx.114",
            "114.xx.xx.115"
        ],
        "availability_zone": "aa-bb-cc",
        "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
        "extra_dhcp_opts": [
            {
                "opt_value": "10.100.0.33,10.100.0.34",
                "opt_name": "ntp"
            }
        ]
    }
}
```

Response Parameters

Table 4-27 Response parameter

Parameter	Type	Description
subnet	**subnet** object	Specifies the **subnet objects**.

Table 4-28 subnet objects

Parameter	Type	Description
id	String	Specifies the resource identifier in the form of UUID.
name	String	• Specifies the subnet name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about the subnet. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	• Specifies the subnet CIDR block. • The value must be within the VPC CIDR block. • The value must be in CIDR format. The subnet mask cannot be greater than 28.

Parameter	Type	Description
gateway_ip	String	• Specifies the gateway of the subnet. • The value must be an IP address in the subnet. • The value must be a valid IP address.
ipv6_enable	Boolean	Specifies whether IPv6 is enabled.
cidr_v6	String	Specifies the IPv6 subnet CIDR block. If the subnet is an IPv4 subnet, this parameter is not returned.
gateway_ip_v6	String	Specifies the IPv6 subnet gateway. If the subnet is an IPv4 subnet, this parameter is not returned.
dhcp_enable	Boolean	Specifies whether DHCP is enabled for the subnet.
primary_dns	String	• Specifies the primary IP address of DNS server on the subnet. • The value must be an IP address. If the value is not specified, the default value will be left blank.
secondary_dns	String	• Specifies the standby IP address of DNS server on the subnet. • The value must be an IP address. If the value is not specified, the default value will be left blank. If only **secondary_dns** is specified and **primary_dns** is not specified, **primary_dns** will automatically use the value of **secondary_dns**. If there is only one DNS server address, only **primary_dns** is displayed.
dnsList	Array of strings	• Specifies the DNS server address list of a subnet. This field is required if you need to use more than two DNS servers. • This parameter value is the superset of both DNS server address 1 and DNS server address 2. If the value is not specified, the default value will be left blank.

Parameter	Type	Description
availability_zone	String	• Specifies the AZ to which the subnet belongs, which can be obtained from endpoints. For details, see **Endpoints**. • The value must be an existing AZ in the system. If the value is not specified, the default value will be left blank.
vpc_id	String	Specifies the ID of the VPC to which the subnet belongs.
status	String	• Specifies the status of the subnet. • The value can be **ACTIVE**, **UNKNOWN**, or **ERROR**. – **ACTIVE**: indicates that the subnet has been associated with a VPC. – **UNKNOWN**: indicates that the subnet has not been associated with a VPC. – **ERROR**: indicates that the subnet is abnormal. • The system creates a subnet and then associates the subnet with a VPC in the threads. In the concurrent scenario, if the CIDR block of the created subnet is the same as that of an existing subnet, the created subnet fails to associate with a VPC after underlying system verification. As a result, the subnet creation fails. • The value of status is **UNKNOWN** before the subnet is associated with a VPC. After the subnet is associated with a VPC in the threads, the status of the subnet is **ACTIVE**.
neutron_network_id	String	Specifies the ID of the corresponding network (OpenStack Neutron API).
neutron_subnet_id	String	Specifies the ID of the corresponding subnet (OpenStack Neutron API).
neutron_subnet_id_v6	String	Specifies the ID of the IPv6 subnet (OpenStack Neutron API). If the subnet is an IPv4 subnet, this parameter is not returned.

Parameter	Type	Description
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the NTP server address or DHCP lease time configured for the subnet. For details, see **Table 4-29**.
scope	String	• Specifies where the subnet is used in edge cloud scenario. • The value can be: – **center**: The subnet is used in a central AZ. – *{azId}*: The subnet is used in an edge AZ.
tenant_id	String	• Project ID
created_at	String	• Specifies the time (UTC) when the subnet is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the subnet is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-29 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	• Specifies the NTP server address or DHCP lease expiration time configured for the subnet. • Constraints: The option **ntp** for **opt_name** indicates the NTP server configured for the subnet. Currently, only IPv4 addresses are supported. A maximum of four IP addresses can be configured, and each address must be unique. Multiple IP addresses must be separated using commas (,). The option **null** for **opt_name** indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. The option **addresstime** for **opt_name** indicates the DHCP lease expiration time of the subnet. The value can be **-1**, which indicates unlimited lease time, or *Number*+**h**. The number ranges from 1 to 30,000. For example, the value can be **5h**. The default value is **24h**.
opt_name	Yes	String	• Specifies the NTP server address or DHCP lease time configured for the subnet. • Currently, the value can only be set to **ntp** or **addresstime**.

Example Response

```
{
    "subnet": {
        "id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
        "name": "subnet",
        "description": "",
        "cidr": "192.168.20.0/24",
        "dnsList": [
            "114.xx.xx.114",
            "114.xx.xx.115"
        ],
        "status": "UNKNOWN",
        "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
```



```
    "gateway_ip": "192.168.20.1",
    "ipv6_enable": true,
    "cidr_v6": "2001:db8:a583::/64",
    "gateway_ip_v6": "2001:db8:a583::1",
    "dhcp_enable": true,
    "primary_dns": "114.xx.xx.114",
    "secondary_dns": "114.xx.xx.115",
    "availability_zone": "aa-bb-cc",
    "neutron_network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
    "neutron_subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
    "neutron_subnet_id_v6": "e0fa7de1-a6e2-44c9-b052-b9d8cebe93c4",
    "extra_dhcp_opts": [
      {
        "opt_value": "10.100.0.33,10.100.0.34",
        "opt_name": "ntp"
      }
    ],
    "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
    "created_at": "2022-12-15T02:42:07",
    "updated_at": "2022-12-15T02:42:07"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.2.2 Querying Subnet Details

Function

This API is used to query details about a subnet.

URI

GET /v1/{project_id}/subnets/{subnet_id}

Table 4-30 describes the parameters.

Table 4-30 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Description
subnet_id	Yes	Specifies the subnet ID, which uniquely identifies the subnet. If you use the management console, the value of this parameter is the **Network ID** value.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/subnets/4779ab1c-7c1a-44b1-a02e-93dfc361b32d
```

Response Parameters

Table 4-31 Response parameter

Parameter	Type	Description
subnet	**subnet** object	Specifies the **subnet objects**.

Table 4-32 subnet objects

Parameter	Type	Description
id	String	Specifies a resource ID in UUID format.
name	String	• Specifies the subnet name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about the subnet. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	Specifies the subnet CIDR block.
gateway_ip	String	Specifies the subnet gateway address.
ipv6_enable	Boolean	Specifies whether IPv6 is enabled.

Parameter	Type	Description
cidr_v6	String	Specifies the IPv6 subnet CIDR block. If the subnet is an IPv4 subnet, this parameter is not returned.
gateway_ip_v6	String	Specifies the IPv6 subnet gateway. If the subnet is an IPv4 subnet, this parameter is not returned.
dhcp_enable	Boolean	Specifies whether DHCP is enabled for the subnet.
primary_dns	String	Specifies the primary IP address of DNS server on the subnet.
secondary_dns	String	Specifies the standby IP address of DNS server on the subnet.
dnsList	Array of strings	Specifies the IP address list of DNS servers on the subnet.
availability_zone	String	Identifies the AZ to which the subnet belongs.
vpc_id	String	Specifies the ID of the VPC to which the subnet belongs.
status	String	• Specifies the status of the subnet. • The value can be **ACTIVE**, **UNKNOWN**, or **ERROR**. – **ACTIVE**: indicates that the subnet has been associated with a VPC. – **UNKNOWN**: indicates that the subnet has not been associated with a VPC. – **ERROR**: indicates that the subnet is abnormal.
neutron_network_id	String	Specifies the ID of the corresponding network (OpenStack Neutron API).
neutron_subnet_id	String	Specifies the ID of the corresponding subnet (OpenStack Neutron API).
neutron_subnet_id_v6	String	Specifies the ID of the IPv6 subnet (OpenStack Neutron API). If the subnet is an IPv4 subnet, this parameter is not returned.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the NTP server address or DHCP lease time configured for the subnet. For details, see **Table 4-33**.

Parameter	Type	Description
scope	String	• Specifies where the subnet is used in edge cloud scenario. • The value can be: – **center**: The subnet is used in a central AZ. – *{azId}*: The subnet is used in an edge AZ.
tenant_id	String	Project ID
created_at	String	• Specifies the time (UTC) when the subnet is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the subnet is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-33 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	• Specifies the NTP server address or DHCP lease expiration time configured for the subnet. • Constraints: The option **ntp** for **opt_name** indicates the NTP server configured for the subnet. Currently, only IPv4 addresses are supported. A maximum of four IP addresses can be configured, and each address must be unique. Multiple IP addresses must be separated using commas (,). The option **null** for **opt_name** indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. The option **addresstime** for **opt_name** indicates the DHCP lease expiration time of the subnet. The value can be **-1**, which indicates unlimited lease time, or *Number*+**h**. The number ranges from 1 to 30,000. For example, the value can be **5h**. The default value is **24h**.
opt_name	Yes	String	• Specifies the NTP server address or DHCP lease time configured for the subnet. • Currently, the value can only be set to **ntp** or **addresstime**.

Example Response

```
{
    "subnet": {
        "id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
        "name": "subnet",
        "description": "",
        "cidr": "192.168.20.0/24",
        "dnsList": [
            "114.xx.xx.114",
            "114.xx.xx.115"
        ],
        "status": "ACTIVE",
        "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
```



```
    "gateway_ip": "192.168.20.1",
    "ipv6_enable": false,
    "dhcp_enable": true,
    "primary_dns": "114.xx.xx.114",
    "secondary_dns": "114.xx.xx.115",
    "availability_zone": "aa-bb-cc",
    "neutron_network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
    "neutron_subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
    "extra_dhcp_opts": [
      {
        "opt_value": "10.100.0.33,10.100.0.34",
        "opt_name": "ntp"
      }
    ],
    "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
    "created_at": "2022-12-15T02:42:07",
    "updated_at": "2022-12-15T02:42:07"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.2.3 Querying Subnets

Function

This API is used to query subnets using search criteria and to display the subnets in a list.

URI

GET /v1/{project_id}/subnets

Example:

```
GET https://{Endpoint}/v1/{project_id}/subnets?limit=10&marker=4779ab1c-7c1a-44b1-a02e-93dfc361b32d&vpc_id=3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85
```

Table 4-34 describes the parameters.

Table 4-34 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.
vpc_id	No	String	Specifies the VPC ID that is used to query subnets.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/subnets
```


Response Parameters

Table 4-35 Response parameter

Parameter	Type	Description
subnets	Array of **subnet** objects	Specifies the subnet objects.

Table 4-36 subnet objects

Parameter	Type	Description
id	String	Specifies a resource ID in UUID format.
name	String	• Specifies the subnet name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about the subnet. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	Specifies the subnet CIDR block.
gateway_ip	String	Specifies the subnet gateway address.
ipv6_enable	Boolean	Specifies whether IPv6 is enabled.
cidr_v6	String	Specifies the IPv6 subnet CIDR block. If the subnet is an IPv4 subnet, this parameter is not returned.
gateway_ip_v6	String	Specifies the IPv6 subnet gateway address. If the subnet is an IPv4 subnet, this parameter is not returned.
dhcp_enable	Boolean	Specifies whether the DHCP function is enabled for the subnet.
primary_dns	String	Specifies the primary IP address of DNS server on the subnet.
secondary_dns	String	Specifies the standby IP address of DNS server on the subnet.
dnsList	Array of strings	Specifies the IP address list of DNS servers on the subnet.

Parameter	Type	Description
availability_zone	String	Identifies the AZ to which the subnet belongs.
vpc_id	String	Specifies the ID of the VPC to which the subnet belongs.
status	String	• Specifies the status of the subnet. • The value can be **ACTIVE**, **UNKNOWN**, or **ERROR**. – **ACTIVE**: indicates that the subnet has been associated with a VPC. – **UNKNOWN**: indicates that the subnet has not been associated with a VPC. – **ERROR**: indicates that the subnet is abnormal.
neutron_network_id	String	Specifies the ID of the network (OpenStack Neutron API).
neutron_subnet_id	String	Specifies the ID of the subnet (OpenStack Neutron API).
neutron_subnet_id_v6	String	Specifies the ID of the IPv6 subnet (OpenStack Neutron API). If the subnet is an IPv4 subnet, this parameter is not returned.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the NTP server address or DHCP lease time configured for the subnet. For details, see **Table 4-37**.
scope	String	• Specifies where the subnet is used in edge cloud scenario. • The value can be: – **center**: The subnet is used in a central AZ. – *{azId}*: The subnet is used in an edge AZ.
tenant_id	String	• Project ID
created_at	String	• Specifies the time (UTC) when the subnet is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the subnet is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-37 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	• Specifies the NTP server address or DHCP lease expiration time configured for the subnet. • Constraints: The option **ntp** for **opt_name** indicates the NTP server configured for the subnet. Currently, only IPv4 addresses are supported. A maximum of four IP addresses can be configured, and each address must be unique. Multiple IP addresses must be separated using commas (,). The option **null** for **opt_name** indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. The option **addresstime** for **opt_name** indicates the DHCP lease expiration time of the subnet. The value can be **-1**, which indicates unlimited lease time, or *Number*+**h**. The number ranges from 1 to 30,000. For example, the value can be **5h**. The default value is **24h**.
opt_name	Yes	String	• Specifies the NTP server address or DHCP lease time configured for the subnet. • Currently, the value can only be set to **ntp** or **addresstime**.

Example Response

```
{
   "subnets": [
      {
         "id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
         "name": "subnet",
         "description": "",
         "cidr": "192.168.20.0/24",
         "dnsList": [
```



```
            "114.xx.xx.114",
            "114.xx.xx.115"
          ],
          "status": "ACTIVE",
          "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
          "gateway_ip": "192.168.20.1",
          "ipv6_enable": true,
          "cidr_v6": "2001:db8:a583::/64",
          "gateway_ip_v6": "2001:db8:a583::1",
          "dhcp_enable": true,
          "primary_dns": "114.xx.xx.114",
          "secondary_dns": "114.xx.xx.115",
          "availability_zone": "aa-bb-cc",
          "neutron_network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
          "neutron_subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
          "neutron_subnet_id_v6": "e0fa7de1-a6e2-44c9-b052-b9d8cebe93c4",
          "extra_dhcp_opts": [
            {
              "opt_value": "10.100.0.33,10.100.0.34",
              "opt_name": "ntp"
            }
          ],
          "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
          "created_at": "2022-12-15T02:42:07",
          "updated_at": "2022-12-15T02:42:07"
        },
        {
          "id": "531dec0f-3116-411b-a21b-e612e42349fd",
          "name": "Subnet1",
          "description": "",
          "cidr": "192.168.1.0/24",
          "dnsList": [
            "114.xx.xx.114",
            "114.xx.xx.115"
          ],
          "status": "ACTIVE",
          "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
          "gateway_ip": "192.168.1.1",
          "ipv6_enable": false,
          "dhcp_enable": true,
          "primary_dns": "114.xx.xx.114",
          "secondary_dns": "114.xx.xx.115",
          "availability_zone": "aa-bb-cc",
          "neutron_network_id": "531dec0f-3116-411b-a21b-e612e42349fd",
          "neutron_subnet_id": "1aac193-a2ad-f153-d122-12d64c2c1d78",
          "extra_dhcp_opts": [
            {
              "opt_value": "10.100.0.33,10.100.0.34",
              "opt_name": "ntp"
            }
          ],
          "tenant_id": "087679f0aa80d32a2f4ec0172f5e902b",
          "created_at": "2022-12-15T03:41:22",
          "updated_at": "2022-12-15T03:41:22"
        }
    ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.2.4 Updating Subnet Information

Function

This API is used to update information about a subnet.

URI

PUT /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}

Table 4-38 describes the parameters.

Table 4-38 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID of the subnet.
subnet_id	Yes	Specifies the subnet ID that uniquely identifies the subnet. If you use the management console, the value of this parameter is the **Network ID** value.

Request Parameters

Table 4-39 Request parameter

Parameter	Mandatory	Type	Description
subnet	Yes	**subnet** object	Specifies the **subnet objects**.

Table 4-40 subnet objects

Parameter	Mandatory	Type	Description
name	Yes	String	• Specifies the subnet name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	• Provides supplementary information about the subnet. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
ipv6_enable	No	Boolean	• Specifies whether IPv6 is enabled. • The value can be **true** (enabled) or **false** (disabled).
dhcp_enable	No	Boolean	• Specifies whether DHCP is enabled for the subnet. • The value can be **true** (enabled) or **false** (disabled). • If this parameter is left blank, the system automatically sets it to **true** by default. If this parameter is set to **false**, newly created ECSs cannot obtain IP addresses, and usernames and passwords cannot be injected using Cloud-init.
primary_dns	No	String	• Specifies the primary IP address of DNS server on the subnet. • The value must be a valid IP address. For instructions about how to obtain a private DNS server address, see **What Are the Private DNS Server Addresses Provided by the DNS Service?** For instructions about how to DNS server address, see **Querying Name Servers**.

Parameter	Mandatory	Type	Description
secondary_dns	No	String	• Specifies the standby IP address of DNS server on the subnet. • The value must be a valid IP address. The value of **secondary_dns** must be different from that of **primary_dns**. If there is only one DNS server address, only **primary_dns** is displayed. For instructions about how to obtain a private DNS server address, see **What Are the Private DNS Server Addresses Provided by the DNS Service?** For instructions about how to DNS server address, see **Querying Name Servers**.
dnsList	No	Array of strings	• Specifies the DNS server address list of a subnet. This field is required if you need to use more than two DNS servers. • This parameter value is the superset of both DNS server address 1 and DNS server address 2. For instructions about how to obtain a private DNS server address, see **What Are the Private DNS Server Addresses Provided by the DNS Service?** For instructions about how to DNS server address, see **Querying Name Servers**.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the NTP server address or DHCP lease time configured for the subnet. For details, see **Table 4-41**.

Table 4-41 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_value	No	String	• Specifies the NTP server address or DHCP lease expiration time configured for the subnet. • Constraints: The option **ntp** for **opt_name** indicates the NTP server configured for the subnet. Currently, only IPv4 addresses are supported. A maximum of four IP addresses can be configured, and each address must be unique. Multiple IP addresses must be separated using commas (,). The option **null** for **opt_name** indicates that no NTP server is configured for the subnet. The parameter value cannot be an empty string. The option **addresstime** for **opt_name** indicates the DHCP lease expiration time of the subnet. The value can be **-1**, which indicates unlimited lease time, or *Number*+**h**. The number ranges from 1 to 30,000. For example, the value can be **5h**. The default value is **24h**.
opt_name	Yes	String	• Specifies the NTP server address or DHCP lease time configured for the subnet. • Currently, the value can only be set to **ntp** or **addresstime**.

Example Request

- Change the name of the subnet whose ID is 4779ab1c-7c1a-44b1-a02e-93dfc361b32d to **subnet02**, and also change its DNS and DHCP configurations.

```
PUT https://{Endpoint}/v1/{project_id}/vpcs/{vpc_id}/subnets/4779ab1c-7c1a-44b1-a02e-93dfc361b32d

{
    "subnet": {
        "name": "subnet02",
        "ipv6_enable": true,
        "dhcp_enable": false,
        "primary_dns": "114.xx.xx.115",
```



```
    "secondary_dns": "114.xx.xx.116",
    "extra_dhcp_opts": [
      {
        "opt_value": "10.100.0.33,10.100.0.34",
        "opt_name": "ntp"
      }
    ]
  }
}
```

Response Parameters

Table 4-42 Response parameter

Parameter	Type	Description
subnet	**subnet** object	Specifies the **subnet** objects.

Table 4-43 subnet objects

Parameter	Type	Description
id	String	Specifies a resource ID in UUID format.
status	String	• Specifies the status of the subnet. • The value can be **ACTIVE**, **UNKNOWN**, or **ERROR**. – **ACTIVE**: indicates that the subnet has been associated with a VPC. – **UNKNOWN**: indicates that the subnet has not been associated with a VPC. – **ERROR**: indicates that the subnet is abnormal.

Example Response

```
{
  "subnet": {
    "id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
    "status": "ACTIVE"
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.2.5 Deleting a Subnet

Function

This API is used to delete a subnet.

URI

DELETE /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}

Table 4-44 describes the parameters.

Table 4-44 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the ID of the subnet VPC.
subnet_id	Yes	Specifies the subnet ID, which uniquely identifies the subnet. If you use the management console, the value of this parameter is the **Network ID** value.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/{project_id}/vpcs/{vpc_id}/subnets/4779ab1c-7c1a-44b1-a02e-93dfc361b32d
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.3 Quota

4.3.1 Querying Quotas

Function

This API is used to query network resource quotas of a tenant. The network resources include VPCs, subnets, security groups, security group rules, EIPs, and VPNs.

URI

GET /v1/{project_id}/quotas

Example:
GET https://{Endpoint}/v1/{project_id}/quotas?type={type}

Table 4-45 describes the parameters.

Table 4-45 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
type	No	String	• Specifies the resource type. • Values: – **vpc**: VPC – **subnet**: Subnet – **securityGroup**: Security group – **securityGroupRule**: Security group rule – **publicIp**: EIP – **vpn**: VPN – **vpngw**: VPN gateway – **vpcPeer**: VPC peering connection – **loadbalancer**: Load balancer – **listener**: Load balancer listener – **physicalConnect**: Direct Connect connection – **virtualInterface**: Virtual interface – **firewall**: Firewall – **shareBandwidthIP**: IP address added to a shared bandwidth – **shareBandwidth**: Shared bandwidth – **address_group**: IP address group – **flow_log**: VPC fow log – **vpcContainRoutetable**: Number of route tables associated with a VPC – **routetableContainRoutes**: Number of routes in a route table

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/quotas
```


Response Parameters

Table 4-46 Response parameter

Parameter	Type	Description
quotas	**quotas** object	Specifies the quota object. For details, see **Table 4-47**.

Table 4-47 Description of the **quotas** field

Parameter	Type	Description
resources	Array of **resource** objects	Specifies the resource objects. For details, see **Table 4-48**.

Table 4-48 Description of the **resource** field

Parameter	Type	Description
type	String	• Specifies the resource type. • Values: – **vpc**: VPC – **subnet**: Subnet – **securityGroup**: Security group – **securityGroupRule**: Security group rule – **publicIp**: EIP – **vpn**: VPN – **vpngw**: VPN gateway – **vpcPeer**: VPC peering connection – **loadbalancer**: Load balancer – **listener**: Load balancer listener – **physicalConnect**: Direct Connect connection – **virtualInterface**: Virtual interface – **firewall**: Firewall – **shareBandwidthIP**: IP address added to a shared bandwidth – **shareBandwidth**: Shared bandwidth – **address_group**: IP address group – **flow_log**: VPC fow log – **vpcContainRoutetable**: Number of route tables associated with a VPC – **routetableContainRoutes**: Number of routes in a route table
used	Integer	• Specifies the number of created network resources. • The value ranges from **0** to the value of **quota**.
quota	Integer	• Specifies the maximum quota values for the resources. • The value ranges from the default quota value to the maximum quota value.
min	Integer	Specifies the minimum quota value allowed.

NOTE

If value **-1** is returned when you use an API to query your VPC quota, this indicates that the VPC quota is not limited.

Example Response


```
{
   "quotas": {
      "resources": [
         {
            "type": "vpc",
            "used": 4,
            "quota": 150,
            "min": 0
         },
         {
            "type": "subnet",
            "used": 5,
            "quota": 400,
            "min": 0
         },
         {
            "type": "securityGroup",
            "used": 1,
            "quota": 100,
            "min": 0
         },
         {
            "type": "securityGroupRule",
            "used": 6,
            "quota": 5000,
            "min": 0
         },
         {
            "type": "publicIp",
            "used": 2,
            "quota": 10,
            "min": 0
         },
         {
            "type": "vpn",
            "used": 0,
            "quota": 5,
            "min": 0
         },
         {
            "type": "vpngw",
            "used": 0,
            "quota": 2,
            "min": 0
         },
         {
            "type": "vpcPeer",
            "used": 0,
            "quota": 50,
            "min": 0
         },
         {
            "type":"physicalConnect",
            "used":0,
            "quota":10,
            "min":0
         },
         {
            "type":"virtualInterface",
            "used":0,
            "quota":50,
            "min":0
         },
         {
            "type": "firewall",
            "used": 0,
            "quota": 200,
            "min": 0
```



```
        },
        {
            "type": "shareBandwidth",
            "used": 0,
            "quota": 5,
            "min": 0
        },
        {
            "type": "shareBandwidthIP",
            "used": 0,
            "quota": 20,
            "min": 0
        },
        {
            "type": "loadbalancer",
            "used": 0,
            "quota": 10,
            "min": 0
        },
        {
            "type": "listener",
            "used": 0,
            "quota": 10,
            "min": 0
        },
        {
            "type": "flow_log",
            "used": 0,
            "quota": 10,
            "min": 0
        },
        {
            "type": "vpcContainRoutetable",
            "used": 0,
            "quota": 1,
            "min": 0
        },
        {
            "type": "routetableContainRoutes",
            "used": 0,
            "quota": 200,
            "min": 0
        },
        {
            "type": "address_group",
            "used": 0,
            "quota": 50,
            "min": 0
        }
    ]
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.4 Private IP Address

4.4.1 Assigning a Private IP Address

Function

This API is used to assign a private IP address.

URI

POST /v1/{project_id}/privateips

Table 4-49 describes the parameters.

Table 4-49 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-50 Request parameter

Parameter	Mandatory	Type	Description
privateips	Yes	Array of **privateip** objects	Specifies the private IP address objects. For details, see **Table 4-51**.

Table 4-51 Description of the **privateip** field

Parameter	Mandatory	Type	Description
subnet_id	Yes	String	Specifies the ID of the subnet from which IP addresses are assigned. If you use the management console, the value of this parameter is the **Network ID** value.
ip_address	No	String	• Specifies the target IP address. • The value can be an available IP address in the subnet. If it is not specified, the system automatically assigns an IP address.

Example Request

- Assign two private IP addresses from the subnet whose ID is 531dec0f-3116-411b-a21b-e612e42349fd. One IP address is automatically assigned, and the other is specified to 192.168.1.17.

```
POST https://{Endpoint}/v1/{project_id}/privateips

{
  "privateips":
   [
    {
        "subnet_id": "531dec0f-3116-411b-a21b-e612e42349fd"
    },
    {
        "subnet_id": "531dec0f-3116-411b-a21b-e612e42349fd",
         "ip_address": "192.168.1.17"
    }
   ]
}
```

Response Parameters

Table 4-52 Response parameter

Parameter	Type	Description
privateips	Array of **privateip** objects	Specifies the private IP address objects. For details, see **Table 4-53**.

Table 4-53 Description of the **privateip** field

Parameter	Type	Description
status	String	• Specifies the status of the private IP address. • Possible values are as follows: – **ACTIVE** – **DOWN**
id	String	Specifies the ID of the private IP address, which uniquely identifies the private IP address.
subnet_id	String	Specifies the ID of the subnet from which IP addresses are assigned. If you use the management console, the value of this parameter is the **Network ID** value.
tenant_id	String	Specifies the project ID.

Parameter	Type	Description
device_owner	String	• Specifies the resource using the private IP address. The parameter is left blank if it is not used. • The value can be: **network:dhcp**: DHCP service IP address **network:router_interface_distributed**: Gateway IP address **compute:*xxx*** (*xxx* indicates the AZ name. For example, **compute:aa-bb-cc** indicates that the IP address is used by an ECS in the AZ aa-bb-cc.): IP address of an ECS NIC **neutron:VIP_PORT**: Virtual IP address **compute:subeni**: IP address of a supplementary network interface **neutron:LOADBALANCERV2**: IP address of a shared load balancer **neutron:LOADBALANCERV3**: IP address of a dedicated load balancer **network:endpoint_interface**: IP address of a VPC endpoint **network:nat_gateway**: IP address used by a NAT gateway • The value range specifies only the type of private IP addresses supported by the current service.
ip_address	String	Specifies the assigned private IP address.

Example Response

```
{
   "privateips": [
      {
         "status": "DOWN",
         "id": "c60c2ce1-1e73-44bd-bf48-fd688448ff7b",
         "subnet_id": "531dec0f-3116-411b-a21b-e612e42349fd",
         "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
         "device_owner": "",
         "ip_address": "192.168.1.10"
      },
      {
         "status": "DOWN",
         "id": "4b123c18-ae92-4dfa-92cd-d44002359aa1",
         "subnet_id": "531dec0f-3116-411b-a21b-e612e42349fd",
         "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
         "device_owner": "",
```



```
        "ip_address": "192.168.1.17"
    }
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.4.2 Querying Private IP Address Details

Function

This API is used to query details about a private IP address using the specified ID.

URI

GET /v1/{project_id}/privateips/{privateip_id}

Table 4-54 describes the parameters.

Table 4-54 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
privateip_id	Yes	Specifies the ID of the private IP address, which uniquely identifies the private IP address.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/privateips/d600542a-b231-45ed-af05-e9930cb14f78
```


Response Parameters

Table 4-55 Response parameter

Parameter	Type	Description
privateip	**privateip** object	Specifies the private IP address objects. For details, see **Table 4-56**.

Table 4-56 Description of the **privateip** field

Parameter	Type	Description
status	String	• Specifies the status of the private IP address. • Possible values are as follows: – **ACTIVE** – **DOWN**
id	String	Specifies the ID of the private IP address, which uniquely identifies the private IP address.
subnet_id	String	Specifies the ID of the subnet from which IP addresses are assigned. If you use the management console, the value of this parameter is the **Network ID** value.
tenant_id	String	Specifies the project ID.

Parameter	Type	Description
device_owner	String	• Specifies the resource using the private IP address. The parameter is left blank if it is not used. • The value can be: **network:dhcp**: DHCP service IP address **network:router_interface_distributed**: Gateway IP address **compute:***xxx* (*xxx* indicates the AZ name. For example, **compute:aa-bb-cc** indicates that the IP address is used by an ECS in the AZ aa-bb-cc.): IP address of an ECS NIC **neutron:VIP_PORT**: Virtual IP address **compute:subeni**: IP address of a supplementary network interface **neutron:LOADBALANCERV2**: IP address of a shared load balancer **neutron:LOADBALANCERV3**: IP address of a dedicated load balancer **network:endpoint_interface**: IP address of a VPC endpoint **network:nat_gateway**: IP address used by a NAT gateway • The value range specifies only the type of private IP addresses supported by the current service.
ip_address	String	Specifies the assigned private IP address.

Example Response

```
{
   "privateip":
      {
         "status": "DOWN",
         "id": "d600542a-b231-45ed-af05-e9930cb14f78",
         "subnet_id": "531dec0f-3116-411b-a21b-e612e42349fd",
         "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
         "device_owner": "",
         "ip_address": "192.168.1.11"
      }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.4.3 Querying Private IP Addresses

Function

This API is used to query private IP addresses using search criteria and to display the private IP addresses in a list.

URI

GET /v1/{project_id}/subnets/{subnet_id}/privateips

Example:

```
GET https://{Endpoint}/v1/{project_id}/subnets/{subnet_id}/privateips?
limit=10&marker=4779ab1c-7c1a-44b1-a02e-93dfc361b32d
```

Table 4-57 describes the parameters.

Table 4-57 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
subnet_id	Yes	String	Specifies the unique ID of the subnet to which the private IP address belongs. If you use the management console, the value of this parameter is the **Network ID** value.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/subnets/{subnet_id}/privateips
```


Response Parameters

Table 4-58 Request parameter

Parameter	Type	Description
privateips	Array of **privateip** objects	Specifies the private IP address objects. For details, see **Table 4-59**.

Table 4-59 Description of the **privateip** field

Parameter	Type	Description
status	String	• Specifies the status of the private IP address. • Possible values are as follows: – **ACTIVE** – **DOWN**
id	String	Specifies the ID of the private IP address, which uniquely identifies the private IP address.
subnet_id	String	Specifies the ID of the subnet from which IP addresses are assigned. If you use the management console, the value of this parameter is the **Network ID** value.
tenant_id	String	Specifies the project ID.

Parameter	Type	Description
device_owner	String	• Specifies the resource using the private IP address. The parameter is left blank if it is not used. • The value can be: **network:dhcp**: DHCP service IP address **network:router_interface_distributed**: Gateway IP address **compute:*xxx*** (*xxx* indicates the AZ name. For example, **compute:aa-bb-cc** indicates that the IP address is used by an ECS in the AZ aa-bb-cc.): IP address of an ECS NIC **neutron:VIP_PORT**: Virtual IP address **compute:subeni**: IP address of a supplementary network interface **neutron:LOADBALANCERV2**: IP address of a shared load balancer **neutron:LOADBALANCERV3**: IP address of a dedicated load balancer **network:endpoint_interface**: IP address of a VPC endpoint **network:nat_gateway**: IP address used by a NAT gateway • The value range specifies only the type of private IP addresses supported by the current service.
ip_address	String	Specifies the assigned private IP address.

Example Response

```
{
  "privateips": [
    {
      "status": "DOWN",
      "id": "d600542a-b231-45ed-af05-e9930cb14f78",
      "subnet_id": "531dec0f-3116-411b-a21b-e612e42349fd",
      "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
      "device_owner": "",
      "ip_address": "192.168.1.11"
    },
    {
      "status": "DOWN",
      "id": "d600542a-b231-45ed-af05-e9930cb14f79",
      "subnet_id": "531dec0f-3116-411b-a21b-e612e42349fd",
      "tenant_id": "8b7e35ad379141fc9df3e178bd64f55c",
      "device_owner": "",
      "ip_address": "192.168.1.12"
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.4.4 Deleting a Private IP Address

Function

This API is used to delete a private IP address.

URI

DELETE /v1/{project_id}/privateips/{privateip_id}

Table 4-60 describes the parameters.

Table 4-60 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
privateip_id	Yes	Specifies the ID of the private IP address, which uniquely identifies the private IP address.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/{project_id}/privateips/4779ab1c-7c1a-44b1-a02e-93dfc361b32d
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.5 Security Group

4.5.1 Creating a Security Group

Function

This API is used to create a security group.

URI

POST /v1/{project_id}/security-groups

Table 4-61 describes the parameters.

Table 4-61 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-62 Request parameter

Parameter	Mandatory	Type	Description
security_group	Yes	**security_group** object	Specifies the security group objects. For details, see **Table 4-63**.

Table 4-63 Description of **security_group** fields

Parameter	Mandatory	Type	Description
name	Yes	String	• Specifies the security group name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Mandatory	Type	Description
vpc_id	No	String	Specifies the ID of the VPC that the security group is associated with. **NOTE** Currently, this parameter is not recommended because it is only used as a prompt and does not restrict that the security group must be associated with the VPC.
enterprise_project_id	No	String	• Specifies the enterprise project ID. When creating a security group, associate the enterprise project ID with the security group. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.

Example Request

- Create a security group named **sg-01** in the VPC with ID of 3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85.

```
POST https://{Endpoint}/v1/{project_id}/security-groups

{
    "security_group": {
        "name": "sg-01",
        "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
        "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
    }
}
```

Response Parameters

Table 4-64 Response parameter

Parameter	Type	Description
security_group	**security_group** object	Specifies the security group objects. For details, see **Table 4-65**.

Table 4-65 Description of **security_group** fields

Parameter	Type	Description
name	String	Specifies the security group name.
description	String	Provides supplementary information about the security group.
id	String	Specifies the security group ID, which uniquely identifies the security group.
vpc_id	String	Specifies the ID of the VPC that the security group is associated with. **NOTE** Currently, this parameter is not recommended because it is only used as a prompt and does not restrict that the security group must be associated with the VPC.
security_group_rules	Array of **security_group_rule** objects	Specifies the default security group rules, which ensure that resources in the security group can communicate with one another.
enterprise_project_id	String	• Specifies the enterprise project ID. When creating a security group, associate the enterprise project ID with the security group. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.

Table 4-66 security_group_rule objects

Parameter	Type	Description
id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
description	String	• Provides supplementary information about the security group rule. • The value can contain no more than 255 characters, including letters and digits.
security_group_id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
direction	String	• Specifies the direction of access control. • Possible values are as follows: – **egress** – **ingress**
ethertype	String	• Specifies the IP protocol version. • The value can be **IPv4** or **IPv6**.
protocol	String	• Specifies the protocol type. • The value can be **icmp**, **tcp**, **udp**, or an IP protocol number (0 to 255, for example, 47 for GRE) • If the parameter is left blank, all protocols are supported.
port_range_min	Integer	• Specifies the start port number. • The value ranges from 1 to 65535. • The value cannot be greater than the **port_range_max** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.

Parameter	Type	Description
port_range_max	Integer	• Specifies the end port number. • The value ranges from 1 to 65535. • If the protocol is not **icmp**, the value cannot be smaller than the **port_range_min** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
remote_ip_prefix	String	• Specifies the remote IP address. If the access control direction is set to **egress**, the parameter specifies the source IP address. If the access control direction is set to **ingress**, the parameter specifies the destination IP address. • The value can be in the CIDR format or IP addresses. • The parameter is mutually exclusive with parameter **remote_group_id** and **remote_address_group_id**.
remote_group_id	String	• Specifies the ID of the peer security group. • The value is mutually exclusive with parameter **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
tenant_id	String	• Specifies the ID of the project to which the security group rule belongs.

Example Response

```
{
    "security_group": {
        "id": "16b6e77a-08fa-42c7-aa8b-106c048884e6",
```



```
    "name": "qq",
    "description": "",
    "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
    "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
    "security_group_rules": [
      {
          "id": "f11a3824-ac19-4fad-b4f1-c5f4a6dd0a80",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "direction": "ingress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv6",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      },
      {
          "id": "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": null,
          "direction": "egress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv6",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      },
      {
          "id": "9581f18c-1fdd-43da-ace9-7758a56ef28a",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": null,
          "direction": "egress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv4",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      },
      {
          "id": "a3ba270e-e58b-432d-a912-aeb7eace9fb8",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "direction": "ingress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv4",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      }
    ]
  }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

4.5.2 Querying Security Group Details

Function

This API is used to query details about a security group.

URI

GET /v1/{project_id}/security-groups/{security_group_id}

Table 4-67 describes the parameters.

Table 4-67 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
security_group_id	Yes	Specifies the security group ID, which uniquely identifies the security group.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/security-groups/16b6e77a-08fa-42c7-aa8b-106c048884e6
```

Response Parameters

Table 4-68 Response parameter

Parameter	Type	Description
security_group	**security_group** object	Specifies the security group object.

Table 4-69 Description of **security_group** fields

Parameter	Type	Description
name	String	Specifies the security group name.
description	String	Provides supplementary information about the security group.
id	String	Specifies the security group ID, which uniquely identifies the security group.
vpc_id	String	Specifies the resource ID of the VPC to which the security group belongs. **NOTE** Currently, this parameter is not recommended because it is only used as a prompt and does not restrict that the security group must be associated with the VPC.
security_group_rules	Array of **security_group_rule** objects	Specifies the default security group rules, which ensure that resources in the security group can communicate with one another.
enterprise_project_id	String	• Specifies the enterprise project ID. When creating a security group, associate the enterprise project ID with the security group. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE**

Table 4-70 security_group_rule objects

Parameter	Type	Description
id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.

Parameter	Type	Description
description	String	• Provides supplementary information about the security group rule. • The value can contain no more than 255 characters, including letters and digits.
security_group_id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
direction	String	• Specifies the direction of access control. • Possible values are as follows: – **egress** – **ingress**
ethertype	String	• Specifies the IP protocol version. • The value can be **IPv4** or **IPv6**.
protocol	String	• Specifies the protocol type. • The value can be **icmp**, **tcp**, **udp**, or an IP protocol number (0 to 255, for example, 47 for GRE) • If the parameter is left blank, all protocols are supported.
port_range_min	Integer	• Specifies the start port number. • The value ranges from 1 to 65535. • The value cannot be greater than the **port_range_max** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.

Parameter	Type	Description
port_range_max	Integer	• Specifies the end port number. • The value ranges from 1 to 65535. • If the protocol is not **icmp**, the value cannot be smaller than the **port_range_min** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
remote_ip_prefix	String	• Specifies the remote IP address. If the access control direction is set to **egress**, the parameter specifies the source IP address. If the access control direction is set to **ingress**, the parameter specifies the destination IP address. • The value can be in the CIDR format or IP addresses. • The parameter is mutually exclusive with parameter **remote_group_id** and **remote_address_group_id**.
remote_group_id	String	• Specifies the ID of the peer security group. • The value is mutually exclusive with parameter **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
tenant_id	String	• Specifies the ID of the project to which the security group rule belongs.

Example Response

```
{
    "security_group": {
        "id": "16b6e77a-08fa-42c7-aa8b-106c048884e6",
```



```
    "name": "qq",
    "description": "qq",
    "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
    "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
    "security_group_rules": [
      {
          "id": "f11a3824-ac19-4fad-b4f1-c5f4a6dd0a80",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "direction": "ingress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv6",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      },
      {
          "id": "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": null,
          "direction": "egress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv6",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      },
      {
          "id": "9581f18c-1fdd-43da-ace9-7758a56ef28a",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": null,
          "direction": "egress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv4",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      },
      {
          "id": "a3ba270e-e58b-432d-a912-aeb7eace9fb8",
          "tenant_id": "060576782980d5762f9ec014dd2f1148",
          "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
          "direction": "ingress",
          "protocol": null,
          "description": "",
          "ethertype": "IPv4",
          "remote_ip_prefix": null,
          "remote_address_group_id": null,
          "port_range_max": null,
          "port_range_min": null
      }
    ]
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.5.3 Querying Security Groups

Function

This API is used to query security groups using search criteria and to display the security groups in a list.

URI

GET /v1/{project_id}/security-groups

Example:

```
GET https://{Endpoint}/v1/{project_id}/security-groups?limit=10&marker=4779ab1c-7c1a-44b1-a02e-93dfc361b32d&vpc_id=3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85
```

Table 4-71 describes the parameters.

Table 4-71 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.
vpc_id	No	String	Specifies that the VPC ID is used as the filtering condition.
enterprise_project_id	No	String	• Specifies the enterprise project ID. This field can be used to filter the security groups of an enterprise project. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. To obtain the security groups bound to all enterprise projects of the user or to display the security group list for enterprise project member accounts, set **all_granted_eps**. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.

Parameter	Mandatory	Type	Description
remote_address_group_id	No	String	• Specifies the remote IP address group ID. You can log in to the management console and view the ID on the IP address group page. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/security-groups
```

Response Parameters

Table 4-72 Response parameter

Parameter	Type	Description
security_groups	Array of **security_group** objects	Specifies the security group objects. For details, see **Table 4-73**.

Table 4-73 Description of **security_group** fields

Parameter	Type	Description
name	String	Specifies the security group name.
description	String	Provides supplementary information about the security group.
id	String	Specifies the security group ID, which uniquely identifies the security group.

Parameter	Type	Description
vpc_id	String	Specifies the ID of the VPC that the security group is associated with. **NOTE** Currently, this parameter is not recommended because it is only used as a prompt and does not restrict that the security group must be associated with the VPC.
security_group_rules	Array of **security_group_rule** objects	Specifies the default security group rules, which ensure that resources in the security group can communicate with one another.
enterprise_project_id	String	• Specifies the enterprise project ID. When creating a security group, associate the enterprise project ID with the security group. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. **NOTE**

Table 4-74 security_group_rule objects

Parameter	Type	Description
id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
description	String	• Provides supplementary information about the security group rule. • The value can contain no more than 255 characters, including letters and digits.
security_group_id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.

Parameter	Type	Description
direction	String	• Specifies the direction of access control. • Possible values are as follows: – **egress** – **ingress**
ethertype	String	• Specifies the IP protocol version. • The value can be **IPv4** or **IPv6**.
protocol	String	• Specifies the protocol type. • The value can be **icmp**, **tcp**, **udp**, or an IP protocol number (0 to 255, for example, 47 for GRE) • If the parameter is left blank, all protocols are supported.
port_range_min	Integer	• Specifies the start port number. • The value ranges from 1 to 65535. • The value cannot be greater than the **port_range_max** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
port_range_max	Integer	• Specifies the end port number. • The value ranges from 1 to 65535. • If the protocol is not **icmp**, the value cannot be smaller than the **port_range_min** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.

Parameter	Type	Description
remote_ip_prefix	String	• Specifies the remote IP address. If the access control direction is set to **egress**, the parameter specifies the source IP address. If the access control direction is set to **ingress**, the parameter specifies the destination IP address. • The value can be in the CIDR format or IP addresses. • The parameter is mutually exclusive with parameter **remote_group_id** and **remote_address_group_id**.
remote_group_id	String	• Specifies the ID of the peer security group. • The value is mutually exclusive with parameter **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
tenant_id	String	• Specifies the ID of the project to which the security group rule belongs.

Example Response


```
{
   "security_groups": [
      {
         "id": "16b6e77a-08fa-42c7-aa8b-106c048884e6",
         "name": "qq",
         "description": "qq",
         "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
         "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
         "security_group_rules": [
         {
            "id": "f11a3824-ac19-4fad-b4f1-c5f4a6dd0a80",
            "tenant_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "direction": "ingress",
            "protocol": null,
            "description": "",
            "ethertype": "IPv6",
            "remote_ip_prefix": null,
```



```
            "remote_address_group_id": null,
            "port_range_max": null,
            "port_range_min": null
        },
        {
            "id": "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
            "tenant_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": null,
            "direction": "egress",
            "protocol": null,
            "description": "",
            "ethertype": "IPv6",
            "remote_ip_prefix": null,
            "remote_address_group_id": null,
            "port_range_max": null,
            "port_range_min": null
        },
        {
            "id": "9581f18c-1fdd-43da-ace9-7758a56ef28a",
            "tenant_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": null,
            "direction": "egress",
            "protocol": null,
            "description": "",
            "ethertype": "IPv4",
            "remote_ip_prefix": null,
            "remote_address_group_id": null,
            "port_range_max": null,
            "port_range_min": null
        },
        {
            "id": "a3ba270e-e58b-432d-a912-aeb7eace9fb8",
            "tenant_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "direction": "ingress",
            "protocol": null,
            "description": "",
            "ethertype": "IPv4",
            "remote_ip_prefix": null,
            "remote_address_group_id": null,
            "port_range_max": null,
            "port_range_min": null
        }
    ]
},
    {
        "id": "9c0f56be-a9ac-438c-8c57-fce62de19419",
        "name": "default",
        "description": "qq",
        "vpc_id": "13551d6b-755d-4757-b956-536f674975c0",
        "enterprise_project_id": "0",
        "security_group_rules": [
            {
                "direction": "egress",
                "ethertype": "IPv4",
                "id": "95479e0a-e312-4844-b53d-a5e4541b783f",
                "description": "",
                "security_group_id": "9c0f56be-a9ac-438c-8c57-fce62de19419"
            },
            {
                "direction": "ingress",
                "ethertype": "IPv4",
                "id": "0c4a2336-b036-4fa2-bc3c-1a291ed4c431",
                "description": "",
                "remote_group_id": "9c0f56be-a9ac-438c-8c57-fce62de19419",
                "security_group_id": "9c0f56be-a9ac-438c-8c57-fce62de19419"
```

```
        }
      ]
    }
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.5.4 Deleting a Security Group

Function

This API is used to delete a security group.

URI

DELETE /v1/{project_id}/security-groups/{security_group_id}

Table 4-75 describes the parameters.

Table 4-75 Parameter description

Parameter	Mandatory	Description
security_group_id	Yes	Specifies the security group ID, which uniquely identifies the security group.
project_id	No	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/{project_id}/security-groups/0c4a2336-b036-4fa2-bc3c-1a291ed4c431
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.5.5 Creating a Security Group Rule

Function

This API is used to create a security group rule.

URI

POST /v1/{project_id}/security-group-rules

Request Parameters

Table 4-76 Request parameter

Parameter	Mandatory	Type	Description
security_group_rule	Yes	**security_group_rule** object	Specifies the security group rule objects. For details, see **Table 4-77**.

Table 4-77 Description of the **security_group_rule** field

Parameter	Mandatory	Type	Description
security_group_id	Yes	String	Specifies the security group ID.
description	No	String	• Provides supplementary information about the security group rule. • The value can contain no more than 255 characters, including letters and digits.
direction	Yes	String	• Access control direction specified in a security group rule. • The value can be: – **egress** – **ingress**

Parameter	Mandatory	Type	Description
ethertype	No	String	• Specifies the IP protocol version. • The value can be **IPv4** or **IPv6**. • If you do not set this parameter, **IPv4** is used by default.
protocol	No	String	• Specifies the protocol type. • The value can be **icmp**, **tcp**, **udp**, or an IP protocol number (0 to 255, for example, 47 for GRE) • If the parameter is left blank, all protocols are supported.
port_range_min	No	Integer	• Specifies the start port number. • The value ranges from 1 to 65535. • The value cannot be greater than the **port_range_max** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
port_range_max	No	Integer	• Specifies the end port number. • The value ranges from 1 to 65535. • If the protocol is not **icmp**, the value cannot be smaller than the **port_range_min** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.

Parameter	Mandatory	Type	Description
remote_ip_prefix	No	String	• Specifies the remote IP address. If the access control direction is set to **egress**, the parameter specifies the source IP address. If the access control direction is set to **ingress**, the parameter specifies the destination IP address. • The value can be in the CIDR format or IP addresses. • The parameter is mutually exclusive with parameter **remote_group_id** and **remote_address_group_id**.
remote_group_id	No	String	• Specifies the ID of the peer security group. • The value is mutually exclusive with parameter **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	No	String	• Specifies the remote IP address group ID. You can log in to the management console and view the ID on the IP address group page. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.

Example Request

- Create an inbound rule in the security group whose ID is a7734e61-b545-452d-a3cd-0189cbd9747a.

```
POST https://{Endpoint}/v1/{project_id}/security-group-rules

{
    "security_group_rule": {
        "direction": "ingress",
        "port_range_min": "80",
        "ethertype": "IPv4",
        "port_range_max": "80",
```



```
        "protocol": "tcp",
        "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "security_group_id": "a7734e61-b545-452d-a3cd-0189cbd9747a"
    }
}
POST https://{Endpoint}/v1/{project_id}/security-group-rules

{
    "security_group_rule": {
        "direction": "ingress",
        "port_range_min": "80",
        "ethertype": "IPv6",
        "port_range_max": "90",
        "protocol": "tcp",
        "security_group_id": "a7734e61-b545-452d-a3cd-0189cbd9747a"
    }
}
```

Response Parameters

Table 4-78 Response parameter

Parameter	Type	Description
security_group_rule	**security_group_rule** object	Specifies the security group rule objects. For details, see **Table 4-79**.

Table 4-79 security_group_rule objects

Parameter	Type	Description
id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
description	String	• Provides supplementary information about the security group rule. • The value can contain no more than 255 characters, including letters and digits.
security_group_id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
direction	String	• Specifies the direction of access control. • Possible values are as follows: – **egress** – **ingress**

Parameter	Type	Description
ethertype	String	• Specifies the IP protocol version. • The value can be **IPv4** or **IPv6**.
protocol	String	• Specifies the protocol type. • The value can be **icmp**, **tcp**, **udp**, or an IP protocol number (0 to 255, for example, 47 for GRE) • If the parameter is left blank, all protocols are supported.
port_range_min	Integer	• Specifies the start port number. • The value ranges from 1 to 65535. • The value cannot be greater than the **port_range_max** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
port_range_max	Integer	• Specifies the end port number. • The value ranges from 1 to 65535. • If the protocol is not **icmp**, the value cannot be smaller than the **port_range_min** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
remote_ip_prefix	String	• Specifies the remote IP address. If the access control direction is set to **egress**, the parameter specifies the source IP address. If the access control direction is set to **ingress**, the parameter specifies the destination IP address. • The value can be in the CIDR format or IP addresses. • The parameter is mutually exclusive with parameter **remote_group_id** and **remote_address_group_id**.

Parameter	Type	Description
remote_group_id	String	• Specifies the ID of the peer security group. • The value is mutually exclusive with parameter **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
tenant_id	String	• Specifies the ID of the project to which the security group rule belongs.

Example Response

```
{
   "security_group_rule": {
      "direction": "ingress",
      "ethertype": "IPv4",
      "id": "2bc0accf-312e-429a-956e-e4407625eb62",
      "description": "",
      "port_range_max": 80,
      "port_range_min": 80,
      "protocol": "tcp",
      "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
      "remote_ip_prefix": null,
      "security_group_id": "a7734e61-b545-452d-a3cd-0189cbd9747a",
      "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550",
      "remote_address_group_id": null
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.5.6 Querying Security Group Rule Details

Function

This API is used to query details about a security group rule.

URI

GET /v1/{project_id}/security-group-rules/{security_group_rule_id}

Table 4-80 describes the parameters.

Table 4-80 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
security_group_rule_id	Yes	Specifies the security group rule ID, which uniquely identifies the security group rule.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/security-group-rules/2bc0accf-312e-429a-956e-e4407625eb62
```

Response Parameters

Table 4-81 Response parameter

Parameter	Type	Description
security_group_rule	**security_group_rule** object	Specifies the security group rule objects. For details, see **Table 4-82**.

Table 4-82 security_group_rule objects

Parameter	Type	Description
id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.

Parameter	Type	Description
description	String	• Provides supplementary information about the security group rule. • The value can contain no more than 255 characters, including letters and digits.
security_group_id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
direction	String	• Specifies the direction of access control. • Possible values are as follows: – **egress** – **ingress**
ethertype	String	• Specifies the IP protocol version. • The value can be **IPv4** or **IPv6**.
protocol	String	• Specifies the protocol type. • The value can be **icmp**, **tcp**, **udp**, or an IP protocol number (0 to 255, for example, 47 for GRE) • If the parameter is left blank, all protocols are supported.
port_range_min	Integer	• Specifies the start port number. • The value ranges from 1 to 65535. • The value cannot be greater than the **port_range_max** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.

Parameter	Type	Description
port_range_max	Integer	• Specifies the end port number. • The value ranges from 1 to 65535. • If the protocol is not **icmp**, the value cannot be smaller than the **port_range_min** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
remote_ip_prefix	String	• Specifies the remote IP address. If the access control direction is set to **egress**, the parameter specifies the source IP address. If the access control direction is set to **ingress**, the parameter specifies the destination IP address. • The value can be in the CIDR format or IP addresses. • The parameter is mutually exclusive with parameter **remote_group_id** and **remote_address_group_id**.
remote_group_id	String	• Specifies the ID of the peer security group. • The value is mutually exclusive with parameter **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
tenant_id	String	• Specifies the ID of the project to which the security group rule belongs.

Example Response

```
{
    "security_group_rule": {
        "direction": "ingress",
```



```
    "ethertype": "IPv4",
    "id": "2bc0accf-312e-429a-956e-e4407625eb62",
    "description":"",
    "port_range_max": 80,
    "port_range_min": 80,
    "protocol": "tcp",
    "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
    "remote_ip_prefix": null,
    "security_group_id": "a7734e61-b545-452d-a3cd-0189cbd9747a",
    "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550",
    "remote_address_group_id": null
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.5.7 Querying Security Group Rules

Function

This API is used to query security group rules using search criteria and to display the security group rules in a list.

URI

GET /v1/{project_id}/security-group-rules

Example:

```
GET https://{Endpoint}/v1/{project_id}/security-group-rules?security_group_id=a7734e61-b545-452da3cd-0189cbd9747a&limit=10&marker=4779ab1c-7c1a-44b1-a02e-93dfc361b32d
```

Table 4-83 describes the parameters.

Table 4-83 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.
security_group_id	No	String	Specifies the security group ID.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/security-group-rules
```

Response Parameters

Parameter	Type	Description
security_group_rules	Array of **security_group_rule** objects	Specifies the security group rule objects. For details, see **Table 4-84**.

Table 4-84 security_group_rule objects

Parameter	Type	Description
id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
description	String	• Provides supplementary information about the security group rule. • The value can contain no more than 255 characters, including letters and digits.

Parameter	Type	Description
security_group_id	String	Specifies the security group rule ID, which uniquely identifies the security group rule.
direction	String	• Specifies the direction of access control. • Possible values are as follows: – **egress** – **ingress**
ethertype	String	• Specifies the IP protocol version. • The value can be **IPv4** or **IPv6**.
protocol	String	• Specifies the protocol type. • The value can be **icmp**, **tcp**, **udp**, or an IP protocol number (0 to 255, for example, 47 for GRE) • If the parameter is left blank, all protocols are supported.
port_range_min	Integer	• Specifies the start port number. • The value ranges from 1 to 65535. • The value cannot be greater than the **port_range_max** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.
port_range_max	Integer	• Specifies the end port number. • The value ranges from 1 to 65535. • If the protocol is not **icmp**, the value cannot be smaller than the **port_range_min** value. An empty value indicates all ports. If the protocol is **icmp**, the value range is shown in **ICMP-Port Range Relationship Table**.

Parameter	Type	Description
remote_ip_prefix	String	• Specifies the remote IP address. If the access control direction is set to **egress**, the parameter specifies the source IP address. If the access control direction is set to **ingress**, the parameter specifies the destination IP address. • The value can be in the CIDR format or IP addresses. • The parameter is mutually exclusive with parameter **remote_group_id** and **remote_address_group_id**.
remote_group_id	String	• Specifies the ID of the peer security group. • The value is mutually exclusive with parameter **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
tenant_id	String	• Specifies the ID of the project to which the security group rule belongs.

Example Response


```
{
   "security_group_rules": [
      {
         "direction": "egress",
         "ethertype": "IPv6",
         "id": "3c0e45ff-adaf-4124-b083-bf390e5482ff",
         "description": "",
         "port_range_max": null,
         "port_range_min": null,
         "protocol": null,
         "remote_group_id": null,
         "remote_ip_prefix": null,
         "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
         "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550",
         "remote_address_group_id": null
      },
      {
         "direction": "egress",
         "ethertype": "IPv4",
```



```
        "id": "93aa42e5-80db-4581-9391-3a608bd0e448",
        "description": "",
        "port_range_max": null,
        "port_range_min": null,
        "protocol": null,
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550",
        "remote_address_group_id": null
    },
    {
        "direction": "ingress",
        "ethertype": "IPv6",
        "id": "c0b09f00-1d49-4e64-a0a7-8a186d928138",
        "description": "",
        "port_range_max": null,
        "port_range_min": null,
        "protocol": null,
        "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "remote_ip_prefix": null,
        "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550",
        "remote_address_group_id": null
    },
    {
        "direction": "ingress",
        "ethertype": "IPv4",
        "id": "f7d45c89-008e-4bab-88ad-d6811724c51c",
        "description": "",
        "port_range_max": null,
        "port_range_min": null,
        "protocol": null,
        "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "remote_ip_prefix": null,
        "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550",
        "remote_address_group_id": null
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.5.8 Deleting a Security Group Rule

Function

This API is used to delete a security group rule.

URI

DELETE /v1/{project_id}/security-group-rules/{security_group_rule_id}

Table 4-85 describes the parameters.

Table 4-85 Parameter description

Parameter	Mandatory	Description
security_group_rule_id	Yes	Specifies the security group rule ID, which uniquely identifies the security group rule.
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/{project_id}/security-group-rules/2bc0accf-312e-429a-956e-e4407625eb62
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.6 Port

4.6.1 Creating a Port

Function

This API is used to create a port to provide functions such as virtual IP addresses and NICs.

URI

POST /v1/{project_id}/ports

Table 4-86 describes the parameters.

Table 4-86 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-87 Request parameter

Parameter	Mandatory	Type	Description
port	Yes	**port** object	Specifies the port objects. For details, see **Table 4-88**.

Table 4-88 Description of the **port** field

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the port name. • The value can contain up to 255 characters. This parameter is left blank by default.
network_id	Yes	String	• Specifies the ID of the network to which the port belongs. • The network ID must exist. **NOTE** To obtain the network ID: • Method 1: Log in to the VPC console and click the target subnet on the **Subnets** page. You can view the network ID on the displayed page. • Method 2: Call the API for querying subnets. For details, see **Querying Subnets**.
admin_state_up	No	Boolean	• Specifies the administrative state of the port. • The default value is **true**.

Parameter	Mandatory	Type	Description
device_owner	No	String	• Specifies the device to which the port belongs. • Currently, only **""** and **neutron:VIP_PORT** are supported. **neutron:VIP_PORT** indicates the port of a virtual IP address.
fixed_ips	No	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. For details, see **Table 4-89**. • A port supports only one fixed IP address that cannot be changed.
tenant_id	No	String	Specifies the project ID.
security_groups	No	Array of strings	Specifies the UUID of the security group, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. This is an extended attribute.

Parameter	Mandatory	Type	Description
allowed_address_pairs	No	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. An address pair consists of an IP address and a MAC address. This attribute is extended. For details, see parameter **allowed_address_pair** in **Table 4-90**. • The IP address cannot be **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • If the virtual IP address is bound to a cloud server: – The value of **mac_address** can be left blank or set to the MAC address of the NIC bound to the cloud server. – Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 4-91**.

Table 4-89 fixed_ip objects

Parameter	Mandatory	Type	Description
subnet_id	No	String	• Specifies the subnet ID. If you use the management console, the value of this parameter is the **IPv4 Subnet ID** or **IPv6 Subnet ID** value. • You cannot change the parameter value.
ip_address	No	String	• Specifies the port IP address. • You cannot change the parameter value.

Table 4-90 allowed_address_pairs objects

Parameter	Mandatory	Type	Description
ip_address	Yes	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of parameter **allowed_address_pairs** is specified, parameter **ip_address** is mandatory.
mac_address	No	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 4-91 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_name	No	String	Specifies the name of the DHCP option. The value of this parameter can only be 51, indicating the DHCP lease time.
opt_value	No	String	• Specifies the value of the DHCP option. • If the value of **opt_name** is **51**, the value format of **opt_value** is *X*h, indicating that the DHCP lease time is *X* hours. • The value of *X* is **-1** or from **1** to **30000**. If the value is **-1**, the DHCP lease time is infinite.

Example Request

- Create a port. Set its network ID to 28a1c93c-9a5e-4a9f-813b-e495bdef7d34, subnet ID to 06bc2359-d75e-4f96-82f4-313e39c7148c, IP address to 192.168.0.38, and associated security group to f2c5b3fc-b971-4a86-87b9-032586260e3e.

```
POST https://{Endpoint}/v1/{project_id}/ports

{
    "port": {
        "fixed_ips": [
            {
                "ip_address": "192.168.0.38",
                "subnet_id": "06bc2359-d75e-4f96-82f4-313e39c7148c"
            }
        ],
        "network_id": "28a1c93c-9a5e-4a9f-813b-e495bdef7d34",
        "security_groups": [
            "f2c5b3fc-b971-4a86-87b9-032586260e3e"
        ]
    }
}
```

Response Parameters

Table 4-92 Response parameter

Parameter	Type	Description
port	**port** object	Specifies the port objects. For details, see **Table 4-93**.

Table 4-93 Description of the **port** field

Parameter	Type	Description
id	String	Specifies the port ID that uniquely identifies the port.
name	String	• Specifies the port name. • The value can contain up to 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network to which the port belongs. • The network ID must exist. **NOTE** To obtain the network ID: • Method 1: Log in to the VPC console and click the target subnet on the **Subnets** page. You can view the network ID on the displayed page. • Method 2: Call the API for querying subnets. For details, see **Querying Subnets**.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The default value is **true**.
mac_address	String	• Specifies the MAC address of the port. • The MAC address is assigned by the system not specified by users.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. For details, see **Table 4-94**. • In IPv4 scenarios, a port supports only one fixed IP address that cannot be changed. In IPv6 scenarios, a port supports a maximum of two fixed IP addresses that cannot be changed.
device_id	String	• Specifies the ID of the device to which the port belongs. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.

Parameter	Type	Description
device_owner	String	• Specifies the owner of the device to which the port belongs, which can be a DHCP server, router, load balancer, or Nova. • The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). • This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**.
tenant_id	String	Specifies the project ID.
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always **DOWN**. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).

Parameter	Type	Description
allowed_address_pairs	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. An address pair consists of an IP address and a MAC address. For details, see **Table 4-95**. • The IP address cannot be **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of **allowed_address_pairs** is the IP address of the ECS NIC, the port corresponding to the virtual IP address is bound.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 4-96**.
binding:vif_details	**binding:vif_details** object	For details, see **Table 4-97**.

Parameter	Type	Description
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Note: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • **normal** indicates software switching. **direct** indicates SR-IOV PCIe passthrough, which is not supported.
dns_assignment	Array of **dns_assignment** objects	• Specifies the default private network domain name information of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.

Parameter	Type	Description
dns_name	String	• Specifies the default private network DNS name of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_id	String	• Specifies the ID of the instance to which the port belongs, for example, RDS instance ID. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_type	String	• Specifies the type of the instance to which the port belongs, for example, RDS. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
port_security_enabled	Boolean	• Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect.
zone_id	String	Specifies the availability zone to which the port belongs.
enable_efi	Boolean	• Specifies whether to enable **efi**. If **efi** is enabled, the port supports vRoCE. The default value is **false**.
ipv6_bandwidth_id	String	• Specifies the ID of the shared bandwidth associated with the IPv6 NIC. • This parameter is displayed only when the IPv6 NIC is associated with a shared bandwidth.

Table 4-94 fixed_ip object

Parameter	Type	Description
subnet_id	String	• Specifies the subnet ID. If you use the management console, the value of this parameter is the **IPv4 Subnet ID** or **IPv6 Subnet ID** value. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 4-95 allowed_address_pairs objects

Parameter	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
mac_address	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 4-96 extra_dhcp_opt object

Parameter	Type	Description
opt_name	String	Specifies the name of the DHCP option. The value of this parameter can only be 51, indicating the DHCP lease time.
opt_value	String	• Specifies the value of the DHCP option. • If the value of **opt_name** is **51**, the value format of **opt_value** is *X*h, indicating that the DHCP lease time is *X* hours. • The value of *X* is **-1** or from **1** to **30000**. If the value is **-1**, the DHCP lease time is infinite.

Table 4-97 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Table 4-98 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Example Response

```
{
    "port": {
        "id": "d00f9c13-412f-4855-8af3-de5d8c24cd60",
        "name": "test",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
                "subnet_id": "70f2e74b-e660-410a-b754-0ca46744348a",
                "ip_address": "10.128.1.10"
            }
        ],
        "dns_name": "",
        "mac_address": "fa:16:3e:d7:f2:6c",
        "network_id": "5b808927-13c9-4e60-a4f4-ed6ffe225167",
        "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "02b4e8ee-74fa-4a31-802e-5490df11245e"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "enable_efi": false
    }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.6.2 Querying a Port

Function

This API is used to query a single port.

URI

GET /v1/{project_id}/ports/{port_id}

Table 4-99 describes the parameters.

Table 4-99 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
port_id	Yes	Specifies the port ID that uniquely identifies the port.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/ports/d00f9c13-412f-4855-8af3-de5d8c24cd60
```

Response Parameters

Table 4-100 Response parameter

Parameter	Type	Description
port	**port** object	Specifies the port objects. For details, see **Table 4-101**.

Table 4-101 Description of the **port** field

Parameter	Type	Description
id	String	Specifies the port ID that uniquely identifies the port.
name	String	• Specifies the port name. • The value can contain up to 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network that the port belongs to. • The network ID must exist. **NOTE** To obtain the network ID: • Method 1: Log in to the VPC console and click the target subnet on the **Subnets** page. You can view the network ID on the displayed page. • Method 2: Call the API for querying subnets. For details, see **Querying Subnets**.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The default value is **true**.
mac_address	String	• Specifies the port MAC address. • The MAC address is assigned by the system not specified by users.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. For details, see **Table 4-102**. • In IPv4 scenarios, a port supports only one fixed IP address that cannot be changed. In IPv6 scenarios, a port supports a maximum of two fixed IP addresses that cannot be changed.
device_id	String	• Specifies the ID of the device that the port belongs to. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.

Parameter	Type	Description
device_owner	String	• Specifies the owner of the device to which the port belongs, which can be a DHCP server, router, load balancer, or Nova. • The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). • This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**.
tenant_id	String	Specifies the project ID.
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always **DOWN**. • The value can be **ACTIVE**, **BUILD**, or **DOWN**. If the value of **allowed_address_pairs** is the IP address of the ECS NIC, the port corresponding to the virtual IP address is bound.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).

Parameter	Type	Description
allowed_address_pairs	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. An address pair consists of an IP address and a MAC address. For details, see **Table 4-103**. • The IP address cannot be **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 4-104**.
binding:vif_details	**binding:vif_details** object	For details, see **Table 4-105**.

Parameter	Type	Description
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Note: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • The value can be **normal** or **direct**. • **normal** indicates software switching. **direct** indicates SR-IOV PCIe passthrough, which is not supported.
dns_assignment	Array of **dns_assignment** objects	• Specifies the default private domain name information of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.

Parameter	Type	Description
dns_name	String	• Specifies the default private network DNS name of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_id	String	• Specifies the ID of the instance to which the port belongs, for example, RDS instance ID. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_type	String	• Specifies the type of the instance to which the port belongs, for example, RDS. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
port_security_enabled	Boolean	• Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect.
zone_id	String	Specifies the availability zone that the port belongs to.
enable_efi	Boolean	• Specifies whether to enable **efi**. If **efi** is enabled, the port supports vRoCE. The default value is **false**.
ipv6_bandwidth_id	String	• Specifies the ID of the shared bandwidth associated with the IPv6 NIC. • This parameter is displayed only when the IPv6 NIC is associated with a shared bandwidth.

Table 4-102 fixed_ip object

Parameter	Type	Description
subnet_id	String	• Specifies the subnet ID. If you use the management console, the value of this parameter is the **IPv4 Subnet ID** or **IPv6 Subnet ID** value. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 4-103 allowed_address_pairs objects

Parameter	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
mac_address	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 4-104 extra_dhcp_opt object

Parameter	Type	Description
opt_name	String	Specifies the name of the DHCP option. The value of this parameter can only be 51, indicating the DHCP lease time.
opt_value	String	• Specifies the value of the DHCP option. • If the value of **opt_name** is **51**, the value format of **opt_value** is *X*h, indicating that the DHCP lease time is *X* hours. • The value of *X* is **-1** or from **1** to **30000**. If the value is **-1**, the DHCP lease time is infinite.

Table 4-105 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Table 4-106 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Example Response

```
{
    "port": {
        "id": "d00f9c13-412f-4855-8af3-de5d8c24cd60",
        "name": "test",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
                "subnet_id": "70f2e74b-e660-410a-b754-0ca46744348a",
                "ip_address": "10.128.1.10"
            }
        ],
        "dns_name": "",
        "mac_address": "fa:16:3e:d7:f2:6c",
        "network_id": "5b808927-13c9-4e60-a4f4-ed6ffe225167",
        "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "02b4e8ee-74fa-4a31-802e-5490df11245e"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "instance_type": "RDS",
        "instance_id": "03a4e9ee-64eb-4a31-802e-5490df22146c",
        "enable_efi": false
    }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.6.3 Querying Ports

Function

This API is used to query ports.

URI

GET /v1/{project_id}/ports

Example:

```
GET https://{Endpoint}/v1/{project_id}/ports?
id={port_id}&name={port_name}&admin_state_up={is_admin_status_up}&network_id={network_id}&mac_address={port_mac}&device_id={port_device_id}&device_owner={device_owner}&status={port_status}&fixed_ips=ip_address={ip_address}&fixed_ips=subnet_id={subnet_id}&limit=10&marker={marker}
```

Table 4-107 describes the parameters.

Table 4-107 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
id	No	String	• Specifies the port ID that is used as the filter.
name	No	String	• Specifies the port name that is used as the filter. • The value can contain up to 255 characters.
admin_state_up	No	Boolean	• Specifies the administrative state that is used as the filter. • The value can be **true** or **false**.
network_id	No	String	• Specifies the network ID that is used as the filter.

Parameter	Mandatory	Type	Description
mac_address	No	String	• Specifies the MAC address that is used as the filter.
device_id	No	String	• Specifies the device ID that is used as the filter.
device_owner	No	String	• Specifies the device owner that is used as the filter. • For details about value range, see parameter **device_owner** in **Table 4-109**.
status	No	String	• Specifies the status that is used as the filter. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	No	Array of strings	• Specifies the UUID of the security group that is used as the filter.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Parameter	Mandatory	Type	Description
fixed_ips	No	Array of strings	• Specifies the port IP address or the ID of the subnet that the port belongs to that is used as the filter. • The value can be **fixed_ips=ip_address={ip_address}** or **fixed_ips=subnet_id={subnet_id}**. Set *{ip_address}* to an IP address, for example, 192.168.21.22. Set *{subnet_id}* to an IPv4 or IPv6 subnet ID, for example, 011fc878-5521-4654-a1ad-f5b0b5820302.
enterprise_project_id	No	String	• Specifies the enterprise project ID that is used as the filter. • The value can be **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. To obtain the ports bound to all enterprise projects of the user, set **all_granted_eps**. **NOTE** For more information about enterprise projects and how to obtain enterprise project IDs, see the **Enterprise Management User Guide**.
enable_efi	No	Boolean	• Whether **efi** is enabled is used as the filter. • The value can be **true** or **false**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/ports
```

Response Parameters

Table 4-108 Response parameter

Parameter	Type	Description
ports	Array of **port** objects	Specifies the port objects. For details, see **Table 4-109**.

Table 4-109 Description of the **port** field

Parameter	Type	Description
id	String	Specifies the port ID that uniquely identifies the port.
name	String	• Specifies the port name. • The value can contain up to 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network that the port belongs to. • The network ID must exist. **NOTE** To obtain the network ID: • Method 1: Log in to the VPC console and click the target subnet on the **Subnets** page. You can view the network ID on the displayed page. • Method 2: Call the API for querying subnets. For details, see **Querying Subnets**.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The default value is **true**.
mac_address	String	• Specifies the port MAC address. • The MAC address is assigned by the system not specified by users.

Parameter	Type	Description
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. For details, see **Table 4-110**. • In IPv4 scenarios, a port supports only one fixed IP address that cannot be changed. In IPv6 scenarios, a port supports a maximum of two fixed IP addresses that cannot be changed.
device_id	String	• Specifies the ID of the device that the port belongs to. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
device_owner	String	• Specifies the owner of the device to which the port belongs, which can be a DHCP server, router, load balancer, or Nova. • The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). • This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**.
tenant_id	String	Specifies the project ID.

Parameter	Type	Description
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always **DOWN**. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).
allowed_address_pairs	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. An address pair consists of an IP address and a MAC address. For details, see **Table 4-111**. • The IP address cannot be **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of **allowed_address_pairs** is the IP address of the ECS NIC, the port corresponding to the virtual IP address is bound.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 4-112**.
binding:vif_details	**binding:vif_details** object	For details, see **Table 4-113**.

Parameter	Type	Description
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Note: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • **normal** indicates software switching. **direct** indicates SR-IOV PCIe passthrough, which is not supported.
dns_assignment	Array of **dns_assignment** objects	• Specifies the default private domain name information of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.

Parameter	Type	Description
dns_name	String	• Specifies the default private network DNS name of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_id	String	• Specifies the ID of the instance to which the port belongs, for example, RDS instance ID. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_type	String	• Specifies the type of the instance to which the port belongs, for example, RDS. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
port_security_enabled	Boolean	• Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect.
zone_id	String	Specifies the availability zone that the port belongs to.
enable_efi	Boolean	• Specifies whether to enable **efi**. If **efi** is enabled, the port supports vRoCE. The default value is **false**.
ipv6_bandwidth_id	String	• Specifies the ID of the shared bandwidth associated with the IPv6 NIC. • This parameter is displayed only when the IPv6 NIC is associated with a shared bandwidth.

Table 4-110 fixed_ip object

Parameter	Type	Description
subnet_id	String	• Specifies the subnet ID. If you use the management console, the value of this parameter is the **IPv4 Subnet ID** or **IPv6 Subnet ID** value. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 4-111 allowed_address_pairs objects

Parameter	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
mac_address	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 4-112 extra_dhcp_opt object

Parameter	Type	Description
opt_name	String	Specifies the name of the DHCP option. The value of this parameter can only be 51, indicating the DHCP lease time.
opt_value	String	• Specifies the value of the DHCP option. • If the value of **opt_name** is **51**, the value format of **opt_value** is *X*h, indicating that the DHCP lease time is *X* hours. • The value of *X* is **-1** or from **1** to **30000**. If the value is **-1**, the DHCP lease time is infinite.

Table 4-113 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Table 4-114 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Example Response

```
{
   "ports": [
      {
         "id": "d00f9c13-412f-4855-8af3-de5d8c24cd60",
         "name": "test",
         "status": "DOWN",
         "admin_state_up": "true",
         "fixed_ips": [
            {
               "subnet_id": "70f2e74b-e660-410a-b754-0ca46744348a",
               "ip_address": "10.128.1.10"
            }
         ],
         "dns_name": "",
         "mac_address": "fa:16:3e:d7:f2:6c",
         "network_id": "5b808927-13c9-4e60-a4f4-ed6ffe225167",
         "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
         "device_id": "",
         "device_owner": "",
         "security_groups": [
            "02b4e8ee-74fa-4a31-802e-5490df11245e"
         ],
         "extra_dhcp_opts": [],
         "allowed_address_pairs": [],
         "binding:vnic_type": "normal",
         "instance_type": "RDS",
         "instance_id": "03a4e9ee-64eb-4a31-802e-5490df22146c",
         "enable_efi": false
      },
```



```
    {
        "id": "28ba8f45-7636-45e4-8c0a-675d7663717c",
        "name": "test1",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
                "subnet_id": "061d3ca2-bd1f-4bd1-a01d-7a5155328c0e",
                "ip_address": "192.168.10.10"
            }
        ],
        "dns_name": "",
        "mac_address": "fa:16:3e:3d:91:cd",
        "network_id": "be2fe79a-3ee2-4d87-bd71-5afa78a5670d",
        "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "0bfc8687-ca18-4c37-ac84-d2198baba585"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "enable_efi": false
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.6.4 Updating a Port

Function

This API is used to update a port.

URI

PUT /v1/{project_id}/ports/{port_id}

Table 4-115 describes the parameters.

Table 4-115 Parameter description

Parameter	Mandatory	Description
port_id	Yes	Specifies the port ID that uniquely identifies the port.

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Parameter	Mandatory	Type	Description
port	Yes	**port** object	Specifies the port objects. For details, see **Table 4-116**. You must specify at least one attribute when updating a port.

Table 4-116 Description of the **port** field

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the port name. • The value can contain up to 255 characters. This parameter is left blank by default.
security_groups	No	Array of strings	• Specifies the UUID of the security group. This is an extended attribute. • This parameter cannot be left blank.

Parameter	Mandatory	Type	Description
allowed_address_pairs	No	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. An address pair consists of an IP address and a MAC address. For details, see parameter **allow_address_pair** in **Table 4-117**. • The IP address cannot be **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 4-118**.

Table 4-117 allowed_address_pairs objects

Parameter	Mandatory	Type	Description
ip_address	Yes	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of parameter **allowed_address_pairs** is specified, parameter **ip_address** is mandatory.
mac_address	No	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 4-118 extra_dhcp_opt object

Parameter	Mandatory	Type	Description
opt_name	No	String	Specifies the name of the DHCP option. The value of this parameter can only be 51, indicating the DHCP lease time.
opt_value	No	String	• Specifies the value of the DHCP option. • If the value of **opt_name** is **51**, the value format of **opt_value** is *X*h, indicating that the DHCP lease time is *X* hours. • The value of *X* is **-1** or from **1** to **30000**. If the value is **-1**, the DHCP lease time is infinite.

Example Request

- Change the name of the port whose ID is 7204e0da-40de-4207-a536-6f59b84f6f0e to **abc**.

```
PUT https://{Endpoint}/v1/{project_id}/ports/7204e0da-40de-4207-a536-6f59b84f6f0e

{
   "port": {
      "name": "adc"
   }
}
```

Response Parameters

Table 4-119 Response parameter

Parameter	Type	Description
port	**port** object	Specifies the port objects. For details, see **Table 4-120**.

Table 4-120 Description of the **port** field

Parameter	Type	Description
id	String	Specifies the port ID that uniquely identifies the port.
name	String	• Specifies the port name. • The value can contain up to 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network that the port belongs to. • The network ID must exist. **NOTE** To obtain the network ID: • Method 1: Log in to the VPC console and click the target subnet on the **Subnets** page. You can view the network ID on the displayed page. • Method 2: Call the API for querying subnets. For details, see **Querying Subnets**.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The default value is **true**.
mac_address	String	• Specifies the port MAC address. • The MAC address is assigned by the system not specified by users.

Parameter	Type	Description
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For details, see **Table 4-121**. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. • In IPv4 scenarios, a port supports only one fixed IP address that cannot be changed. In IPv6 scenarios, a port supports a maximum of two fixed IP addresses that cannot be changed.
device_id	String	• Specifies the ID of the device that the port belongs to. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
device_owner	String	• Specifies the owner of the device to which the port belongs, which can be a DHCP server, router, load balancer, or Nova. • The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). • This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**.
tenant_id	String	Specifies the project ID.

Parameter	Type	Description
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always **DOWN**. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).
allowed_address_pairs	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. An address pair consists of an IP address and a MAC address. For details, see **Table 4-122**. • The IP address cannot be **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • If the value of **allowed_address_pairs** is the IP address of the ECS NIC, the port corresponding to the virtual IP address is bound. • Set **allowed_address_pairs** of the cloud server NIC to **1.1.1.1/0**.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 4-123**.
binding:vif_details	**binding:vif_details** object	For details, see **Table 4-124**.

Parameter	Type	Description
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Note: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • **normal** indicates software switching. **direct** indicates SR-IOV PCIe passthrough, which is not supported.
dns_assignment	Array of **dns_assignment** objects	• Specifies the default private domain name information of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.

Parameter	Type	Description
dns_name	String	• Specifies the default private network DNS name of the primary NIC. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_id	String	• Specifies the ID of the instance to which the port belongs, for example, RDS instance ID. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
instance_type	String	• Specifies the type of the instance to which the port belongs, for example, RDS. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
port_security_enabled	Boolean	• Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect.
zone_id	String	Specifies the availability zone that the port belongs to.
enable_efi	Boolean	• Specifies whether to enable **efi**. If **efi** is enabled, the port supports vRoCE. The default value is **false**.
ipv6_bandwidth_id	String	• Specifies the ID of the shared bandwidth associated with the IPv6 NIC. • This parameter is displayed only when the IPv6 NIC is associated with a shared bandwidth.

Table 4-121 fixed_ip object

Parameter	Type	Description
subnet_id	String	• Specifies the subnet ID. If you use the management console, the value of this parameter is the **IPv4 Subnet ID** or **IPv6 Subnet ID** value. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 4-122 allowed_address_pairs objects

Parameter	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
mac_address	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 4-123 extra_dhcp_opt object

Parameter	Type	Description
opt_name	String	Specifies the name of the DHCP option. The value of this parameter can only be 51, indicating the DHCP lease time.
opt_value	String	• Specifies the value of the DHCP option. • If the value of **opt_name** is **51**, the value format of **opt_value** is *X*h, indicating that the DHCP lease time is *X* hours. • The value of *X* is **-1** or from **1** to **30000**. If the value is **-1**, the DHCP lease time is infinite.

Table 4-124 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Table 4-125 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Example Response

```
{
    "port": {
        "id": "7204e0da-40de-4207-a536-6f59b84f6f0e",
        "name": "adc",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
                "subnet_id": "689156ca-038f-4478-b265-fd26aa8bbe31",
                "ip_address": "192.168.0.9"
            }
        ],
        "mac_address": "fa:16:3e:d7:f2:6c",
        "network_id": "b4152e98-e3af-4e49-bb7f-7766e2b5ec63",
        "tenant_id": "caa6cf4337ea47fb823b15709ebe8591",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "59b39002-e79b-4bac-8e27-aa884ab1beb6"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "enable_efi": false
    }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.6.5 Deleting a Port

Function

This API is used to delete a port.

Restrictions

- A port with **device_owner** set to a value other than **neutron:VIP_PORT** cannot be deleted.
- A port with **device_id** specified cannot be deleted.

URI

DELETE /v1/{project_id}/ports/{port_id}

Table 4-126 describes the parameters.

Table 4-126 Parameter description

Parameter	Mandatory	Description
port_id	Yes	Specifies the port ID that uniquely identifies the port.
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/{project_id}/ports/d00f9c13-412f-4855-8af3-de5d8c24cd60
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.7 VPC Peering Connection

4.7.1 Querying VPC Peering Connections

Function

This API is used to query all VPC peering connections accessible to the tenant submitting the request. The connections are filtered based on the filtering condition. For details about pagination query, see section **Pagination**.

URI

GET /v2.0/vpc/peerings

Example:

```
GET https://{Endpoint}/v2.0/vpc/peerings?
id={id}&name={name}&status={status}&tenant_id={tenant_id}&vpc_id={vpc_id}&limit={limit}&marker={marker}
```

Table 4-127 describes the parameters.

Table 4-127 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the VPC peering connection ID is used as the filtering condition.
name	No	String	• Specifies that the peering connection name is used as the filter. • The value can contain no more than 64 characters.

Parameter	Mandatory	Type	Description
status	No	String	Specifies that the VPC peering connection status is used as the filtering condition.
tenant_id	No	String	Specifies that the tenant ID is used as the filtering condition.
vpc_id	No	String	Specifies that the VPC ID is used as the filtering condition.
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**. The default value is **2000**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/vpc/peerings
```

Response Parameters

Table 4-128 Response parameter

Parameter	Type	Description
peerings	Array of **peering** objects	Specifies the VPC peering connection object list. For details, see **Table 4-129**.
peerings_links	Array of **peerings_link** objects	Specifies the VPC peering connection object list. For details, see **Table 4-131**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 4-129 peering objects

Attribute	Type	Description
id	String	Specifies the VPC peering connection ID.
name	String	Specifies the VPC peering connection name.

Attribute	Type	Description
status	String	Specifies the VPC peering connection status. Possible values are as follows: • **PENDING_ACCEPTANCE** • **REJECTED** • **EXPIRED** • **DELETED** • **ACTIVE**
request_vpc_info	**vpc_info** object	Specifies information about the local VPC. For details, see **Table 4-130**.
accept_vpc_info	**vpc_info** object	Specifies information about the peer VPC. For details, see **Table 4-130**.
description	String	Provides supplementary information about the VPC peering connection.
created_at	String	• Specifies the time (UTC) when the VPC peering connection is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the VPC peering connection is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-130 vpc_info objects

Attribute	Type	Description
vpc_id	String	Specifies the ID of a VPC involved in a VPC peering connection.
tenant_id	String	Specifies the ID of the project to which a VPC involved in the VPC peering connection belongs.

Table 4-131 peerings_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

```
{
   "peerings": [
      {
         "request_vpc_info": {
            "vpc_id": "9daeac7c-a98f-430f-8e38-67f9c044e299",
            "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
         },
         "accept_vpc_info": {
            "vpc_id": "f583c072-0bb8-4e19-afb2-afb7c1693be5",
            "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
         },
         "name": "test",
         "description": "test",
         "id": "b147a74b-39bb-4c7a-aed5-19cac4c2df13",
         "status": "ACTIVE"
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.7.2 Querying a VPC Peering Connection

Function

This API is used to query details about a VPC peering connection.

URI

GET /v2.0/vpc/peerings/{peering_id}

Table 4-132 describes the parameters.

Table 4-132 Parameter description

Parameter	Mandatory	Type	Description
peering_id	Yes	String	Specifies the VPC peering connection ID, which uniquely identifies the VPC peering connection. The **peering_id** value is used as the filter.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/vpc/peerings/22b76469-08e3-4937-8c1d-7aad34892be1
```

Response Parameters

Table 4-133 Response parameter

Parameter	Type	Description
peering	**peering** object	Specifies the VPC peering connection object list. For details, see **Table 4-134**.

Table 4-134 peering objects

Attribute	Type	Description
id	String	Specifies the VPC peering connection ID.
name	String	Specifies the VPC peering connection name.
status	String	Specifies the VPC peering connection status. Possible values are as follows: • **PENDING_ACCEPTANCE** • **REJECTED** • **EXPIRED** • **DELETED** • **ACTIVE**

Attribute	Type	Description
request_vpc_info	**vpc_info** object	Specifies information about the local VPC. For details, see **Table 4-135**.
accept_vpc_info	**vpc_info** object	Specifies information about the peer VPC. For details, see **Table 4-135**.
description	String	Provides supplementary information about the VPC peering connection.
created_at	String	Specifies the time (UTC) when the VPC peering connection is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-135 vpc_info objects

Attribute	Type	Description
vpc_id	String	Specifies the ID of a VPC involved in a VPC peering connection.
tenant_id	String	Specifies the ID of the project to which a VPC involved in the VPC peering connection belongs.

Example Response

```
{
    "peering": {
        "name": "test",
        "description": "test",
        "id": "22b76469-08e3-4937-8c1d-7aad34892be1",
        "request_vpc_info": {
            "vpc_id": "9daeac7c-a98f-430f-8e38-67f9c044e299",
            "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
        },
        "accept_vpc_info": {
            "vpc_id": "f583c072-0bb8-4e19-afb2-afb7c1693be5",
            "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
        },
        "status": "ACTIVE"
    }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.7.3 Creating a VPC Peering Connection

Function

This API is used to create a VPC peering connection.

If you create a VPC peering connection with another VPC of your own, the connection is created without the need for you to accept the connection.

If you create a VPC peering connection with a VPC of another tenant, the peer tenant must accept the connection so that the connection can be created. If the peer tenant refuses the connection, it cannot be created.

URI

POST /v2.0/vpc/peerings

Request Parameters

Table 4-136 Request parameter

Parameter	Mandatory	Type	Description
peering	Yes	**peering** object	Specifies the VPC peering connection. For details, see **Table 4-137**.

Table 4-137 Description of the **peering** field

Attribute	Mandatory	Type	Description
name	Yes	String	Specifies the name of the VPC peering connection. The value can contain 1 to 64 characters.

Attribute	Mandatory	Type	Description
description	No	String	Provides supplementary information about the VPC peering connection. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
request_vpc_info	Yes	**vpc_info** object	Specifies information about the local VPC. For details, see **Table 4-138**.
accept_vpc_info	Yes	**vpc_info** object	Specifies information about the peer VPC. For details, see **Table 4-138**.

Table 4-138 Description of the **vpc_info** field

Attribute	Mandatory	Type	Description
vpc_id	Yes	String	Specifies the ID of a VPC involved in a VPC peering connection.
tenant_id	No	String	Specifies the ID of the project to which a VPC involved in the VPC peering connection belongs. This parameter is mandatory if the VPC peering connection is created between VPCs in different accounts.

Example Request

- Create a VPC peering connection. The VPC ID of the requester is 9daeac7c-a98f-430f-8e38-67f9c044e299, the VPC ID of the receiver is f583c072-0bb8-4e19-afb2-afb7c1693be5, and the VPC peering connection is named **test**.

```
POST https://{Endpoint}/v2.0/vpc/peerings

{
    "peering": {
        "name": "test",
        "description": "test",
        "request_vpc_info": {
            "vpc_id": "9daeac7c-a98f-430f-8e38-67f9c044e299"
        },
        "accept_vpc_info": {
            "vpc_id": "f583c072-0bb8-4e19-afb2-afb7c1693be5"
```



```
    }
  }
}
```

Response Parameters

Table 4-139 Response parameter

Parameter	Type	Description
peering	peering object	Specifies the VPC peering connection. For details, see Table 4-140.

Table 4-140 peering objects

Attribute	Type	Description
id	String	Specifies the VPC peering connection ID.
name	String	Specifies the VPC peering connection name.
status	String	Specifies the VPC peering connection status. Possible values are as follows: • **PENDING_ACCEPTANCE** • **REJECTED** • **EXPIRED** • **DELETED** • **ACTIVE**
request_vpc_info	vpc_info object	Specifies information about the local VPC. For details, see Table 4-141.
accept_vpc_info	vpc_info object	Specifies information about the peer VPC. For details, see Table 4-141.
description	String	Provides supplementary information about the VPC peering connection.
created_at	String	Specifies the time (UTC) when the VPC peering connection is created. Format: *yyyy-MM-ddTHH:mm:ss*

Attribute	Type	Description
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-141 vpc_info objects

Attribute	Type	Description
vpc_id	String	Specifies the ID of a VPC involved in a VPC peering connection.
tenant_id	String	Specifies the ID of the project to which a VPC involved in the VPC peering connection belongs.

Example Response

```
{
   "peering": {
      "name": "test",
      "id": "22b76469-08e3-4937-8c1d-7aad34892be1",
      "request_vpc_info": {
         "vpc_id": "9daeac7c-a98f-430f-8e38-67f9c044e299",
         "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
      },
      "accept_vpc_info": {
         "vpc_id": "f583c072-0bb8-4e19-afb2-afb7c1693be5",
         "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
      },
      "status": "ACTIVE"
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.7.4 Accepting a VPC Peering Connection

Function

After tenant A requests to create a VPC peering connection with a VPC of tenant B, the VPC peering connection takes effect only after tenant B accepts the request. This API is used by a tenant to accept a VPC peering connection request initiated by another tenant.

URI

PUT /v2.0/vpc/peerings/{peering_id}/accept

Table 4-142 describes the parameters.

Table 4-142 Parameter description

Parameter	Mandatory	Type	Description
peering_id	Yes	String	Specifies the VPC peering connection ID, which uniquely identifies the VPC peering connection.

Request Parameters

None

Example Request

- Accept the VPC peering connection request from 22b76469-08e3-4937-8c1d-7aad34892be1.
  PUT https://{Endpoint}/v2.0/vpc/peerings/22b76469-08e3-4937-8c1d-7aad34892be1/accept

Response Parameters

Table 4-143 Response parameter

Attribute	Type	Description
id	String	Specifies the VPC peering connection ID.
name	String	Specifies the VPC peering connection name.
status	String	Specifies the VPC peering connection status. Possible values are as follows: • **PENDING_ACCEPTANCE** • **REJECTED** • **EXPIRED** • **DELETED** • **ACTIVE**
request_vpc_info	**vpc_info** object	Specifies information about the local VPC. For details, see **Table 4-144**.

Attribute	Type	Description
accept_vpc_info	**vpc_info** object	Specifies information about the peer VPC. For details, see **Table 4-144**.
description	String	Provides supplementary information about the VPC peering connection.
created_at	String	Specifies the time (UTC) when the VPC peering connection is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-144 vpc_info objects

Attribute	Type	Description
vpc_id	String	Specifies the ID of a VPC involved in a VPC peering connection.
tenant_id	String	Specifies the ID of the project that a VPC involved in the VPC peering connection belongs to.

Example Response

```
{
    "name": "test",
    "description": "test",
    "id": "22b76469-08e3-4937-8c1d-7aad34892be1",
    "request_vpc_info": {
        "vpc_id": "9daeac7c-a98f-430f-8e38-67f9c044e299",
        "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
    },
    "accept_vpc_info": {
        "vpc_id": "f583c072-0bb8-4e19-afb2-afb7c1693be5",
        "tenant_id": "059a737356594b41b447b557bf0aae56"
    },
    "status": "ACTIVE"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.7.5 Refusing a VPC Peering Connection

Function

After tenant A requests to create a VPC peering connection with a VPC of tenant B, the VPC peering connection takes effect only after tenant B accepts the request. However, tenant can refuse the VPC peering connection request. This API is used by a tenant to refuse a VPC peering connection request initiated by another tenant.

URI

PUT /v2.0/vpc/peerings/{peering_id}/reject

Table 4-145 describes the parameters.

Table 4-145 Parameter description

Parameter	Mandatory	Type	Description
peering_id	Yes	String	Specifies the VPC peering connection ID, which uniquely identifies the VPC peering connection.

Request Parameters

None

Example Request

- Reject the VPC peering connection request from 22b76469-08e3-4937-8c1d-7aad34892be1.
  PUT https://{Endpoint}/v2.0/vpc/peerings/22b76469-08e3-4937-8c1d-7aad34892be1/reject

Response Parameters

Table 4-146 Response parameter

Attribute	Type	Description
id	String	Specifies the VPC peering connection ID.
name	String	Specifies the VPC peering connection name.

Attribute	Type	Description
status	String	Specifies the VPC peering connection status. Possible values are as follows: • **PENDING_ACCEPTANCE** • **REJECTED** • **EXPIRED** • **DELETED** • **ACTIVE**
request_vpc_info	**vpc_info** object	Specifies information about the local VPC. For details, see **Table 4-147**.
accept_vpc_info	**vpc_info** object	Specifies information about the peer VPC. For details, see **Table 4-147**.
description	String	Provides supplementary information about the VPC peering connection.
created_at	String	Specifies the time (UTC) when the VPC peering connection is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-147 vpc_info objects

Attribute	Type	Description
vpc_id	String	Specifies the ID of a VPC involved in a VPC peering connection.
tenant_id	String	Specifies the ID of the project that a VPC involved in the VPC peering connection belongs to.

Example Response

```
{
  "name": "test",
  "description": "test",
  "id": "22b76469-08e3-4937-8c1d-7aad34892be1",
  "request_vpc_info": {
```



```
    "vpc_id": "9daeac7c-a98f-430f-8e38-67f9c044e299",
    "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
  },
  "accept_vpc_info": {
    "vpc_id": "f583c072-0bb8-4e19-afb2-afb7c1693be5",
    "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
  },
  "status": "REJECTED"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.7.6 Updating a VPC Peering Connection

Function

Updates a VPC peering connection.

URI

PUT /v2.0/vpc/peerings/{peering_id}

Table 4-148 describes the parameters.

Table 4-148 Parameter description

Parameter	Mandatory	Type	Description
peering_id	Yes	String	Specifies the VPC peering connection ID, which uniquely identifies the VPC peering connection.

Request Parameters

Table 4-149 Request parameter

Parameter	Mandatory	Type	Description
peering	Yes	peering object	Updates a VPC peering connection. For details, see Table 4-150. When updating a VPC peering connection, you must specify at least one attribute. Currently, only the VPC peering connection name and description can be updated.

Table 4-150 Description of the **peering** field

Parameter	Mandatory	Type	Description
name	No	String	Specifies the name of the VPC peering connection. The value can contain 1 to 64 characters.
description	No	String	Provides supplementary information about the VPC peering connection. The value can contain no more than 255 characters, including letters and digits.

Example Request

- Change the name of the VPC peering connection whose ID is 7a9a954a-eb41-4954-a300-11ab17a361a2 to **test2**.

```
PUT https://{Endpoint}/v2.0/vpc/peerings/7a9a954a-eb41-4954-a300-11ab17a361a2

{
    "peering": {
        "name": "test2"
    }
}
```

Response Parameters

Table 4-151 Response parameter

Parameter	Type	Description
peering	peering object	Specifies the VPC peering connection. For details, see Table 4-152.

Table 4-152 peering objects

Attribute	Type	Description
id	String	Specifies the VPC peering connection ID.
name	String	Specifies the VPC peering connection name.
status	String	Specifies the VPC peering connection status. Possible values are as follows: • **PENDING_ACCEPTANCE** • **REJECTED** • **EXPIRED** • **DELETED** • **ACTIVE**
request_vpc_info	**vpc_info** object	Specifies information about the local VPC. For details, see **Table 4-153**.
accept_vpc_info	**vpc_info** object	Specifies information about the peer VPC. For details, see **Table 4-153**.
description	String	Provides supplementary information about the VPC peering connection.
created_at	String	Specifies the time (UTC) when the VPC peering connection is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the VPC peering connection is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-153 vpc_info objects

Attribute	Type	Description
vpc_id	String	Specifies the ID of a VPC involved in a VPC peering connection.
tenant_id	String	Specifies the ID of the project that a VPC involved in the VPC peering connection belongs to.

Example Response

```
{
   "peering": {
      "name": "test2",
      "description": "test",
      "id": "22b76469-08e3-4937-8c1d-7aad34892be1",
      "request_vpc_info": {
         "vpc_id": "9daeac7c-a98f-430f-8e38-67f9c044e299",
         "tenant_id": "f65e9ebc-ed5d-418b-a931-9a723718ba4e"
      },
      "accept_vpc_info": {
         "vpc_id": "f583c072-0bb8-4e19-afb2-afb7c1693be5",
         "tenant_id": "059a737356594b41b447b557bf0aae56"
      },
      "status": "ACTIVE"
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.7.7 Deleting a VPC Peering Connection

Function

This API is used to delete a VPC peering connection.

A VPC peering connection can be deleted either by the local or peer tenant.

URI

DELETE /v2.0/vpc/peerings/{peering_id}

Table 4-154 describes the parameters.

Table 4-154 Parameter description

Parameter	Mandatory	Type	Description
peering_id	Yes	String	Specifies the VPC peering connection ID, which uniquely identifies the VPC peering connection.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/vpc/peerings/2b098395-046a-4071-b009-312bcee665cb
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.8 VPC Route

4.8.1 Querying VPC Routes

Function

This API is used to query all routes of the tenant submitting the request. The routes are filtered based on the filtering condition. For details about the response format of pagination query, see section **Pagination**.

URI

GET /v2.0/vpc/routes

Example:

```
Example:
GET https://{Endpoint}/v2.0/vpc/routes?
id={id}&vpc_id={vpc_id}&tenant_id={tenant_id}&destination={destination}&type={type}&limit={limit}&marke
r={marker}
```

Table 4-155 describes the parameters.

Table 4-155 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the route ID is used as the filtering condition.

Parameter	Mandatory	Type	Description
tenant_id	No	String	Specifies that the tenant ID is used as the filtering condition.
vpc_id	No	String	Specifies that the VPC ID is used as the filtering condition.
destination	No	String	Specifies that the route destination address (CIDR) is used as the filtering condition.
type	No	String	Specifies that the type is used as the filtering condition. Currently, the value can only be **peering**.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**. The default value is **2000**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/vpc/routes?vpc_id=ab78be2d-782f-42a5-aa72-35879f6890ff
```

Response Parameters

Table 4-156 Response parameter

Parameter	Type	Description
routes	Array of **route** objects	Specifies the route object list. For details, see **Table 4-157**.
routes_links	Array of **routes_link** objects	Specifies the route object list. For details, see **Table 4-158**. The value of **rel** will be **next** and that of **href** will be a link only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**).

Table 4-157 route objects

Attribute	Type	Description
id	String	Specifies the route ID.
destination	String	Specifies the destination address in the CIDR notation format, for example, 192.168.200.0/24.
nexthop	String	Specifies the next hop. If the route type is **peering**, enter the VPC peering connection ID.
type	String	Specifies the route type. Currently, the value can only be **peering**.
vpc_id	String	Specifies the VPC of the route. Set this parameter to the existing VPC ID.
tenant_id	String	Specifies the project ID.

Table 4-158 routes_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

```
{
  "routes": [
    {
      "type": "peering",
      "nexthop": "60c809cb-6731-45d0-ace8-3bf5626421a9",
      "destination": "192.168.200.0/24",
      "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
      "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
      "id": "3d42a0d4-a980-4613-ae76-a2cddecff054"
    }
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.8.2 Querying a VPC Route

Function

This API is used to query details about a route.

URI

GET /v2.0/vpc/routes/{route_id}

Table 4-159 describes the parameters.

Table 4-159 Parameter description

Parameter	Mandatory	Type	Description
route_id	Yes	String	Specifies the route ID, which uniquely identifies the route.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/vpc/routes/60c809cb-6731-45d0-ace8-3bf5626421a9
```

Response Parameters

Table 4-160 Response parameter

Parameter	Type	Description
route	**route** object	Specifies the route. For details, see **Table 4-161**.

Table 4-161 route objects

Attribute	Type	Description
id	String	Specifies the route ID.
destination	String	Specifies the destination address in the CIDR notation format, for example, 192.168.200.0/24.
nexthop	String	Specifies the next hop. If the route type is **peering**, enter the VPC peering connection ID.
type	String	Specifies the route type. Currently, the value can only be **peering**.
vpc_id	String	Specifies the VPC of the route. Set this parameter to the existing VPC ID.
tenant_id	String	Specifies the project ID.

Example Response

```
{
    "route": {
        "type": "peering",
        "nexthop": "60c809cb-6731-45d0-ace8-3bf5626421a9",
        "destination": "192.168.200.0/24",
        "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
        "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
        "id": "3d42a0d4-a980-4613-ae76-a2cddecff054"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.8.3 Creating a VPC Route

Function

This API is used to create a route.

URI

POST /v2.0/vpc/routes

Request Parameters

Table 4-162 Request parameter

Parameter	Type	Mandatory	Description
route	**route** object	Yes	Specifies the route. For details, see **Table 4-163**.

Table 4-163 route objects

Attribute	Type	Mandatory	Description
destination	String	Yes	Specifies the destination address in the CIDR notation format, for example, 192.168.200.0/24. Both IPv4 and IPv6 addresses are supported.
nexthop	String	Yes	Specifies the next hop. If the route type is **peering**, enter the VPC peering connection ID. For details about how to obtain the VPC peering connection ID, see **Querying VPC Peering Connections**.

Attribute	Type	Mandatory	Description
type	String	Yes	Specifies the route type. Currently, only the **peering** type is supported, that is, the next hop is a VPC peering connection. If the next hop is an ECS, do not use this API. Refer to **Updating a Route Table**.
vpc_id	String	Yes	Specifies the ID of the VPC ID requesting for creating a route.

Example Request

- Create a route in the route table of the VPC whose ID is ab78be2d-782f-42a5-aa72-35879f6890ff for the VPC peering connection. The next hop is the peering connection whose ID is 60c809cb-6731-45d0-ace8-3bf5626421a9, and the destination is 192.168.200.0/24.

```
POST https://{Endpoint}/v2.0/vpc/routes

{
    "route": {
        "type": "peering",
        "nexthop": "60c809cb-6731-45d0-ace8-3bf5626421a9",
        "destination": "192.168.200.0/24",
        "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff"
    }
}
```

Response Parameters

Table 4-164 Response parameter

Parameter	Type	Description
route	**route** object	Specifies the route. For details, see **Table 4-165**.

Table 4-165 route objects

Attribute	Type	Description
id	String	Specifies the route ID.
destination	String	Specifies the destination address in the CIDR notation format, for example, 192.168.200.0/24.

Attribute	Type	Description
nexthop	String	Specifies the next hop. If the route type is **peering**, enter the VPC peering connection ID.
type	String	Specifies the route type. Currently, the value can only be **peering**.
vpc_id	String	Specifies the VPC of the route. Set this parameter to the existing VPC ID.
tenant_id	String	Specifies the project ID.

Example Response

```
{
   "route": {
      "type": "peering",
      "nexthop": "60c809cb-6731-45d0-ace8-3bf5626421a9",
      "destination": "192.168.200.0/24",
      "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
      "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
      "id": "3d42a0d4-a980-4613-ae76-a2cddecff054"
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.8.4 Deleting a VPC Route

Function

This API is used to delete a route.

URI

DELETE /v2.0/vpc/routes/{route_id}

Table 4-166 describes the parameters.

Table 4-166 Parameter description

Parameter	Mandatory	Type	Description
route_id	Yes	String	Specifies the route ID, which uniquely identifies the route.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/vpc/routes/60c809cb-6731-45d0-ace8-3bf5626421a9
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.9 Route Table

4.9.1 Querying Route Tables

Function

This API is used to query route tables.

URI

GET /v1/{project_id}/routetables

Example:

```
GET https://{Endpoint}/v1/{project_id}/routetables?limit=10&marker=4779ab1c-7c1a-44b1-a02e-93dfc361b32d&vpc_id=3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85&subnet_id=9873b33f-ac1c-4630-ad1c-7dba1ed79r78
```

Table 4-167 describes the parameters.

Table 4-167 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.

Parameter	Mandatory	Type	Description
id	No	String	Specifies the route table ID that is used as the filter.
vpc_id	No	String	Specifies the VPC UUID that is used as the filter.
subnet_id	No	String	Specifies the subnet UUID that is used as the filter. If you use the management console, the value of this parameter is the **Network ID** value.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/{project_id}/routetables?limit=10&marker=4779ab1c-7c1a-44b1-a02e-93dfc361b32d&vpc_id=3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85&subnet_id=9873b33f-ac1c-4630-ad1c-7dba1ed79r78
```

Response Parameters

Table 4-168 Response parameter

Parameter	Type	Description
routetables	Array of **routetable** objects	Specifies the route table list. For details, see **Table 4-169**.

Table 4-169 Description of the **routetable** field

Parameter	Type	Description
id	String	• Specifies the route table ID that uniquely identifies a route table. • The value must be in standard UUID format.
name	String	• Specifies the route table name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
default	Boolean	• Specifies whether the route table is the default one. • The value can be **true** (default route table) or **false** (custom route table).
subnets	Array of **subnet** objects	• Specifies the subnets associated with the route table. For details, see **Table 4-170**. • Only subnets in the VPC to which the route table belongs can be associated with the route table.
tenant_id	String	• Specifies the project ID.
vpc_id	String	• Specifies the ID of the VPC associated with the route table.
description	String	• Provides supplementary information about the route table. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
created_at	String	• Specifies the time (UTC) when the route table is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the route table is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-170 Description of the **subnet** field

Parameter	Type	Description
id	String	Specifies the ID of the subnet associated with the route table.

Example Response

```
{
  "routetables": [
    {
      "id": "3d42a0d4-a980-4613-ae76-a2cddecff054",
      "name": "routetable-1234",
      "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
      "subnets": [
        {
          "id": "8d4ce32f-d68a-4c4c-9f18-c68d8a5c7f2f"
        }
      ],
```



```
        "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
        "description": "abc",
        "created_at": "2022-12-15T02:56:40",
        "updated_at": "2022-12-15T02:56:40"
    },
    {
        "id": "3d42a0d4-a980-4613-ae76-a2cddecfff89",
        "name": "routetable-5678",
        "vpc_id": "ab78be2d-782f-42a5-aa72-35879f667809",
        "subnets": [
            {
                "id": "8d4ce32f-d68a-4c4c-9f18-c68d8a5c7f2f"
            }
        ],
        "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
        "description": "abc",
        "created_at": "2022-12-15T02:59:03",
        "updated_at": "2022-12-15T02:59:03"
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.9.2 Querying a Route Table

Function

This API is used to query details about a route table.

URI

GET /v1/{project_id}/routetables/{routetable_id}

Table 4-171 describes the parameters.

Table 4-171 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
routetable_id	Yes	String	Specifies the route table ID that uniquely identifies a route table.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/26ae5181a416420998eb2093aaed84d9/routetables/66df8c1f-d4f6-4a63-9abb-09701fe27b39
```

Response Parameters

Table 4-172 Response parameter

Parameter	Type	Description
routetable	**routetable** object	Specifies the route table. For details, see **Table 4-173**.

Table 4-173 Description of the **routetable** field

Parameter	Type	Description
id	String	• Specifies the route table ID that uniquely identifies the route table. • The value must be in standard UUID format.
name	String	• Specifies the route table name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
default	Boolean	• Specifies whether the route table is the default one. • The value can be **true** (default route table) or **false** (custom route table).
routes	Array of **route** objects	• Specifies the route list. For details, see **Table 4-174**. • Each route table can have a maximum of 200 routes.
subnets	Array of **subnet** objects	• Specifies the subnets associated with the route table. For details, see **Table 4-175**. • Only subnets in the VPC to which the route table belongs can be associated with the route table.
tenant_id	String	• Specifies the project ID.

Parameter	Type	Description
vpc_id	String	• Specifies the ID of the VPC associated with the route table.
description	String	• Provides supplementary information about the route table. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
created_at	String	• Specifies the time (UTC) when the route table is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the route table is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-174 Description of the **route** field

Parameter	Type	Description
type	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Type	Description
nexthop	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.
description	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Table 4-175 Description of the **subnet** field

Parameter	Type	Description
id	String	Specifies the ID of the subnet associated with the route table.

Example Response

```
{
 "routetable": {
  "id": "05250d7e-0396-4fc9-9c9c-e4d5594784e4",
```



```
 "name": "rtb-vpc-l2cg-1",
 "routes": [
  {
   "type": "local",
   "destination": "192.168.4.0/24",
   "nexthop": "-"
  },
  {
   "type": "local",
   "destination": "192.168.1.0/24",
   "nexthop": "-"
  },
  {
   "type": "local",
   "destination": "198.19.128.0/20",
   "nexthop": "-"
  },
  {
   "type": "local",
   "destination": "127.0.0.0/8",
   "nexthop": "-"
  },
  {
   "type": "local",
   "destination": "100.64.0.0/10",
   "nexthop": "-"
  }
 ],
 "subnets": [
  {
   "id": "0e0faa8f-ea73-47aa-b919-8c133e98d5ac"
  },
  {
   "id": "e007e005-10aa-4614-b439-c9a14e55130e"
  }
 ],
 "vpc_id": "7978e43c-f892-49d8-9fab-9bb90a51709b",
 "default": true,
 "tenant_id": "05e369f07a800f802f41c002632ba5f9",
 "created_at": "2022-12-15T02:56:40",
 "updated_at": "2022-12-15T02:56:40"
}
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.9.3 Creating a Route Table

Function

This API is used to create a route table.

Notes and Constraints

- The destination CIDR block of a custom route table cannot be included in the CIDR blocks of the local route.
- Each destination CIDR block of a route in the same route table must be unique.

- No more than five routes can be created at a time.

URI

POST /v1/{project_id}/routetables

Table 4-176 describes the parameters.

Table 4-176 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-177 Request parameter

Parameter	Mandatory	Type	Description
routetable	Yes	**routetable** object	Specifies the route table. For details, see **Table 4-178**.

Table 4-178 Description of the **routetable** field

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the route table name. • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
routes	No	Array of **route** objects	• Specifies the route list. For details, see **Table 4-179**. • Each route table can have a maximum of 200 routes.
vpc_id	Yes	String	• Specifies the ID of the VPC associated with the route table.

Parameter	Mandatory	Type	Description
description	No	String	• Provides supplementary information about the route table. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Table 4-179 Description of the **route** field

Parameter	Mandatory	Type	Description
type	Yes	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	Yes	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Mandatory	Type	Description
nexthop	Yes	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.
description	No	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Example Request

- Create a route table named **routetable-1234** for the VPC whose ID is 60c809cb-6731-45d0-ace8-3bf5626421a9 and create a route with next hop type of ECS.

```
POST https://{Endpoint}/v1/6fbe9263116a4b68818cf1edce16bc4f/routetables

{
   "routetable": {
      "name": "routetable-1234",
      "vpc_id": "60c809cb-6731-45d0-ace8-3bf5626421a9",
      "routes":[
        {
          "type": "ecs",
          "destination": "10.10.10.0/24",
          "nexthop":"7c50463d-d36c-4417-aa85-cc11fa10f341"
        }
      ],
      "description":"abc"
   }
}
```

Response Parameters

Table 4-180 Response parameter

Parameter	Type	Description
routetable	**routetable** object	Specifies the route table. For details, see **Table 4-181**.

Table 4-181 Description of the **routetable** field

Parameter	Type	Description
id	String	• Specifies the route table ID that uniquely identifies the route table. • The value must be in standard UUID format.
name	String	• Specifies the route table name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
default	Boolean	• Specifies whether the route table is the default one. • The value can be **true** (default route table) or **false** (custom route table).
routes	Array of **route** objects	• Specifies the route list. For details, see **Table 4-174**. • Each route table can have a maximum of 200 routes.

Parameter	Type	Description
subnets	Array of **subnet** objects	• Specifies the subnets associated with the route table. For details, see **Table 4-175**. • Only subnets in the VPC to which the route table belongs can be associated with the route table.
tenant_id	String	• Specifies the project ID.
vpc_id	String	• Specifies the ID of the VPC associated with the route table.
description	String	• Provides supplementary information about the route table. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
created_at	String	• Specifies the time (UTC) when the route table is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the route table is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-182 Description of the **route** field

Parameter	Type	Description
type	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Type	Description
nexthop	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.
description	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Table 4-183 Description of the **subnet** field

Parameter	Type	Description
id	String	Specifies the ID of the subnet associated with the route table.

Example Response

```
{
    "routetable": {
        "id": "3d42a0d4-a980-4613-ae76-a2cddecff054",
```



```
    "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
    "description": "abc",
    "routes": [
      {
        "type": "ecs",
        "destination": "10.10.10.0/24",
        "nexthop": "7c50463d-d36c-4417-aa85-cc11fa10f341",
        "description": "abc"
      }
    ],
    "subnets": [
      {
        "id": "8d4ce32f-d68a-4c4c-9f18-c68d8a5c7f2f"
      }
    ],
    "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
    "created_at": "2022-12-15T02:56:40",
    "updated_at": "2022-12-15T02:56:40"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.9.4 Updating a Route Table

Function

This API is used to update a route table.

URI

PUT /v1/{project_id}/routetables/{routetable_id}

Table 4-184 describes the parameters.

Table 4-184 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
routetable_id	Yes	String	Specifies the route table ID that uniquely identifies a route table.

Request Parameters

Table 4-185 Request parameter

Parameter	Mandatory	Type	Description
routetable	Yes	**routetable** object	Specifies the route table. For details, see **Table 4-186**.

Table 4-186 Description of the **routetable** field

Parameter	Mandatory	Type	Description
name	No	String	• Specifies the route table name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Parameter	Mandatory	Type	Description
routes	No	RouteTableRouteAction object	• Specifies the route list. For details, see Table 4-187. • Constraints: – Each route table can have a maximum of 200 routes. – The destination cannot be modified directly. To modify the destination, run the **del** command to delete the corresponding route, and then run the **add** command to add a route. • Specifies the operation to perform. Possible values are as follows: – **add**: Adds a route. Parameters **type**, **destination**, and **nexthop** are mandatory. – **mod**: Modifies a route. Parameters **type**, **destination**, and **nexthop** are mandatory. – **del**: Deletes a route. Parameter **destination** is mandatory.

Table 4-187 Description of the **route** field

Parameter	Mandatory	Type	Description
add	No	Array of AddRouteTableRoute objects	Adds a route. For details, see Table 4-188. Parameters **type**, **destination**, and **nexthop** are mandatory.
mod	No	Array of ModRouteTableRoute objects	Modifies a route. For details, see Table 4-189. Parameters **type**, **destination**, and **nexthop** are mandatory.

Parameter	Mandatory	Type	Description
del	No	Array of **DelRouteTableRoute** objects	Deletes a route. For details, see **Table 4-190**. Parameter **destination** is mandatory.

Table 4-188 Field description of adding a route

Parameter	Mandatory	Type	Description
type	Yes	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	Yes	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Mandatory	Type	Description
nexthop	Yes	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.
description	No	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Table 4-189 Field description of modifying a route

Parameter	Mandatory	Type	Description
type	Yes	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	Yes	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Mandatory	Type	Description
nexthop	Yes	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.

Parameter	Mandatory	Type	Description
description	No	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Table 4-190 Field description of deleting a route

Parameter	Mandatory	Type	Description
type	No	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.

Parameter	Mandatory	Type	Description
destination	Yes	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Mandatory	Type	Description
nexthop	No	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.

Parameter	Mandatory	Type	Description
description	No	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Example Request

- Change the route table whose ID is 3d42a0d4-a980-4613-ae76-a2cddecff054, add a route with next hop type of ECS, modify the route with next hop type of ECS, and delete the route whose destination is 20.20.10.0/24.

```
PUT https://{Endpoint}/v1/6fbe9263116a4b68818cf1edce16bc4f/routetables/3d42a0d4-a980-4613-ae76-a2cddecff054

{
   "routetable": {
      "name": "routertable-789",
      "description": "abc",
      "routes": {
         "add": [
            {
               "type": "ecs",
               "destination": "10.10.10.0/24",
               "nexthop": "7c50463d-d36c-4417-aa85-cc11fa10f341",
               "description": "abc"
            }
         ],
         "mod": [
            {
               "type": "ecs",
               "destination": "20.10.10.0/24",
               "nexthop": "7c50463d-d36c-4417-aa85-cc11fa10f341",
               "description": "abc"
            }
         ],
         "del": [
            {
               "destination": "20.20.10.0/24"
            }
         ]
      }
   }
}
```

Response Parameters

Table 4-191 Response parameter

Parameter	Type	Description
routetable	**routetable** object	Specifies the route table. For details, see **Table 4-192**.

Table 4-192 Description of the **routetable** field

Parameter	Type	Description
id	String	• Specifies the route table ID that uniquely identifies the route table. • The value must be in standard UUID format.
name	String	• Specifies the route table name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
default	Boolean	• Specifies whether the route table is the default one. • The value can be **true** (default route table) or **false** (custom route table).
routes	Array of **route** objects	• Specifies the route list. For details, see **Table 4-174**. • Each route table can have a maximum of 200 routes.
subnets	Array of **subnet** objects	• Specifies the subnets associated with the route table. For details, see **Table 4-175**. • Only subnets in the VPC to which the route table belongs can be associated with the route table.
tenant_id	String	• Specifies the project ID.
vpc_id	String	• Specifies the ID of the VPC associated with the route table.
description	String	• Provides supplementary information about the route table. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
created_at	String	• Specifies the time (UTC) when the route table is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the route table is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-193 Description of the **route** field

Parameter	Type	Description
type	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Type	Description
nexthop	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.
description	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Table 4-194 Description of the **subnet** field

Parameter	Type	Description
id	String	Specifies the ID of the subnet associated with the route table.

Example Response

```
{
    "routetable": {
        "id": "3d42a0d4-a980-4613-ae76-a2cddecff054",
```



```
    "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
    "description": "abc",
    "default": false,
    "routes": [
      {
        "type": "ecs",
        "destination": "10.10.10.0/24",
        "nexthop": "7c50463d-d36c-4417-aa85-cc11fa10f341",
        "description": "abc"
      }
    ],
    "subnets": [
      {
        "id": "8d4ce32f-d68a-4c4c-9f18-c68d8a5c7f2f"
      }
    ],
    "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
    "created_at": "2022-12-15T02:56:40",
    "updated_at": "2022-12-15T03:03:42"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.9.5 Associating Subnets with a Route Table

Function

This API is used to associate a subnet with a route table.

If a subnet has already been associated with route table A, you can associate the subnet with route table B directly without disassociating it from route table A first.

URI

POST /v1/{project_id}/routetables/{routetable_id}/action

Table 4-195 describes the parameters.

Table 4-195 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
routetable_id	Yes	String	Specifies the route table ID, which uniquely identifies a route table.

Request Parameters

Table 4-196 Request parameter

Parameter	Mandatory	Type	Description
routetable	Yes	**routetable** object	Specifies the route table. For details, see **Table 4-197**.

Table 4-197 Description of the **routetable** field

Parameter	Mandatory	Type	Description
subnets	Yes	**subnet** object	• Specifies the subnets associated with the route table. • Only subnets in the VPC that the route table belongs to can be associated with the route table.

Table 4-198 Description of the **subnet** field

Parameter	Mandatory	Type	Description
associate	No	Array of strings	Specifies a list of IDs of the subnets to be associated with the route table.
disassociate	No	Array of strings	Specifies a list of IDs of the subnets to be disassociated from the route table.

Example Request

- Associate route table 3d42a0d4-a980-4613-ae76-a2cddecff054 with subnet 1a8b8c98-3976-401b-a735-8b058109268c.

  ```
  POST https://{Endpoint}/v1/6fbe9263116a4b68818cf1edce16bc4f/routetables/3d42a0d4-a980-4613-ae76-a2cddecff054/action
  ```



```
{
   "routetable": {
      "subnets": {
         "associate": [
            "1a8b8c98-3976-401b-a735-8b058109268c"
         ]
      }
   }
}
```

Response Parameters

Table 4-199 Response parameter

Parameter	Type	Description
routetable	**routetable** object	Specifies the route table. For details, see **Table 4-200**.

Table 4-200 Description of the **routetable** field

Parameter	Type	Description
id	String	• Specifies the route table ID, which uniquely identifies the route table. • The value must be in standard UUID format.
name	String	• Specifies the route table name. • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
default	Boolean	• Specifies whether the route table is the default one. • The value can be **true** (default route table) or **false** (custom route table).
routes	Array of **route** objects	• Specifies the route list. For details, see **Table 4-201**. • Each route table can have a maximum of 200 routes.
subnets	Array of **subnet** objects	• Specifies the subnets associated with the route table. For details, see **Table 4-202**. • Only subnets in the VPC to which the route table belongs can be associated with the route table.
tenant_id	String	• Specifies the project ID.

Parameter	Type	Description
vpc_id	String	• Specifies the ID of the VPC associated with the route table.
description	String	• Provides supplementary information about the route table. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
created_at	String	• Specifies the time (UTC) when the route table is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the route table is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-201 Description of the **route** field

Parameter	Type	Description
type	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Type	Description
nexthop	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.
description	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Table 4-202 Description of the **subnet** field

Parameter	Type	Description
id	String	Specifies the ID of the subnet associated with the route table.

Example Response

```
{
    "routetable": {
        "id": "3d42a0d4-a980-4613-ae76-a2cddecff054",
```



```
    "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
    "description": "abc",
    "routes": [
      {
        "type": "ecs",
        "destination": "10.10.10.0/24",
        "nexthop": "7c50463d-d36c-4417-aa85-cc11fa10f341",
        "description": "abc"
      }
    ],
    "subnets": [
      {
        "id": "8d4ce32f-d68a-4c4c-9f18-c68d8a5c7f2f"
      }
    ],
    "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
    "created_at": "2022-12-15T02:56:40",
    "updated_at": "2022-12-15T03:05:10"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.9.6 Disassociating Subnets from a Route Table

Function

This API is used to disassociate subnets from a route table.

URI

POST /v1/{project_id}/routetables/{routetable_id}/action

Table 4-203 describes the parameters.

Table 4-203 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
routetable_id	Yes	String	Specifies the route table ID, which uniquely identifies a route table.

Request Parameters

Table 4-204 Request parameter

Parameter	Mandatory	Type	Description
routetable	Yes	**routetable** object	Specifies the route table. For details, see **Table 4-205**.

Table 4-205 Description of the **routetable** field

Parameter	Mandatory	Type	Description
subnets	Yes	**subnet** object	• Specifies the subnets associated with the route table. • Only subnets in the VPC that the route table belongs to can be associated with the route table.

Table 4-206 Description of the **subnet** field

Parameter	Mandatory	Type	Description
associate	No	Array of strings	Specifies the IDs of the subnets to be associated with the route table.
disassociate	No	Array of strings	Specifies the IDs of the subnets to be disassociated from the route table.

Example Request

- Disassociate route table 3d42a0d4-a980-4613-ae76-a2cddecff054 from subnet 815a6b9e-f766-48eb-967c-0ada72d85435.

```
POST https://{Endpoint}/v1/6fbe9263116a4b68818cf1edce16bc4f/routetables/3d42a0d4-a980-4613-ae76-a2cddecff054/action

{
    "routetable": {
        "subnets": {
            "disassociate": [
                "815a6b9e-f766-48eb-967c-0ada72d85435"
            ]
        }
    }
}
```

Response Parameters

Table 4-207 Response parameter

Parameter	Type	Description
routetable	**routetable** object	Specifies the route table. For details, see **Table 4-208**.

Table 4-208 Description of the **routetable** field

Parameter	Type	Description
id	String	• Specifies the route table ID, which uniquely identifies the route table. • The value must be in standard UUID format.
name	String	• Specifies the route table name. • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
default	Boolean	• Specifies whether the route table is the default one. • The value can be **true** (default route table) or **false** (custom route table).
routes	Array of **route** objects	• Specifies the route list. For details, see **Table 4-209**. • Each route table can have a maximum of 200 routes.
subnets	Array of **subnet** objects	• Specifies the subnets associated with the route table. For details, see **Table 4-210**. • Only subnets in the VPC to which the route table belongs can be associated with the route table.
tenant_id	String	• Specifies the project ID.
vpc_id	String	• Specifies the ID of the VPC associated with the route table.
description	String	• Provides supplementary information about the route table. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
created_at	String	• Specifies the time (UTC) when the route table is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the route table is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 4-209 Description of the **route** field

Parameter	Type	Description
type	String	• Specifies the route type. • Values: – **ecs** (ECS) – **eni** (NIC) – **vip** (Virtual IP address) – **nat** (NAT gateway) – **peering** (VPC peering connection) – **vpn** (VPN) – **dc** (Direct Connect connection) – **cc** (Cloud Connect connection) – **egw**: VPC endpoint node – **er**: enterprise router – **subeni**: supplementary network interface. – **local**: reserved CIDR block. The destination CIDR block of the route configured cannot overlap with that defined by **local**.
destination	String	• Specifies the destination CIDR block of a route. • Constraints: The value must be in valid IPv4 or IPv6 CIDR formats.

Parameter	Type	Description
nexthop	String	• Specifies the ID of the next hop in the route. • Values: – When **type** is **ecs**, the value is an ECS ID. – When **type** is **eni**, the value is an extension NIC ID. – When **type** is **vip**, the value is a virtual IP address. – When **type** is **nat**, the value a NAT gateway ID. – When **type** is **peering**, the value is a VPC peering connection ID. – When **type** is **vpn**, the value is a VPN ID. – When **type** is **dc**, the value is a Direct Connect connection ID. – When **type** is **cc**, the value is a Cloud Connect connection ID. – When **type** is set to **egw**, the value is a VPC endpoint ID. – When **type** is set to **er**, the value is the ID of an enterprise router. – When **type** is set to **subeni**, the value is the ID of a supplementary network interface.
description	String	• Provides supplementary information about the route. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Table 4-210 Description of the **subnet** field

Parameter	Type	Description
id	String	Specifies the ID of the subnet associated with the route table.

Example Response

```
{
    "routetable": {
        "id": "3d42a0d4-a980-4613-ae76-a2cddecff054",
```



```
    "vpc_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
    "description": "abc",
    "routes": [
      {
        "type": "ecs",
        "destination": "10.10.10.0/24",
        "nexthop": "7c50463d-d36c-4417-aa85-cc11fa10f341",
        "description": "abc"
      }
    ],
    "subnets": [
      {
        "id": "8d4ce32f-d68a-4c4c-9f18-c68d8a5c7f2f"
      }
    ],
    "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
    "created_at": "2022-12-15T02:56:40",
    "updated_at": "2022-12-15T03:06:21"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.9.7 Deleting a Route Table

Function

This API is used to delete a custom route table.

Constraints:

Only custom route tables can be deleted. If a custom route table has subnets associated, disassociate the subnets with the route table and then delete the route table.

URI

DELETE /v1/{project_id}/routetables/{routetable_id}

Table 4-211 describes the parameters.

Table 4-211 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
routetable_id	Yes	String	Specifies the route table ID, which uniquely identifies a route table.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/{project_id}/routetables/3d42a0d4-a980-4613-ae76-a2cddecff054
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.10 VPC Tag Management

4.10.1 Adding a Tag to a VPC

Function

This API is used to add a tag to a VPC.

URI

POST /v2.0/{project_id}/vpcs/{vpc_id}/tags

Table 4-212 describes the parameters.

Table 4-212 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID that uniquely identifies the VPC.

Request Parameters

Table 4-213 Request parameter

Parameter	Type	Mandatory	Description
tag	**tag** object	Yes	Specifies the **tag** objects. For details, see **Table 4-214**.

Table 4-214 tag objects

Attribute	Type	Mandatory	Description
key	String	Yes	• Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-). • The tag key of a VPC must be unique.
value	String	Yes	• Specifies the tag value. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Request

- Create a tag for a VPC. The key is **key1**, and the value is **value1**.


```
POST https://{Endpoint}/v2.0/{project_id}/vpcs/{vpc_id}/tags

{
    "tag": {
        "key": "key1",
        "value": "value1"
    }
}
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.10.2 Querying VPC Tags

Function

This API is used to query tags of a specified VPC.

URI

GET /v2.0/{project_id}/vpcs/{vpc_id}/tags

Table 4-215 describes the parameters.

Table 4-215 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID that uniquely identifies the VPC.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/{project_id}/vpcs/{vpc_id}/tags
```

Response Parameters

Table 4-216 Response parameter

Parameter	Type	Description
tags	Array of **tag** objects	Specifies the **tag** object list. For details, see **Table 4-217**.

Table 4-217 tag objects

Attribute	Type	Description
key	String	• Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-). • The tag key of a VPC must be unique.
value	String	• Specifies the tag value. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Response

```
{
  "tags": [
    {
      "key": "key1",
      "value": "value1"
    },
    {
      "key": "key2",
      "value": "value3"
    }
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.10.3 Deleting a Tag from a VPC

Function

This API is used to delete a tag from a VPC.

URI

DELETE /v2.0/{project_id}/vpcs/{vpc_id}/tags/{key}

Table 4-218 describes the parameters.

Table 4-218 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID, which uniquely identifies the VPC.
key	Yes	Specifies the tag key.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/{project_id}/vpcs/{vpc_id}/tags/{key}
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.10.4 Batch Adding or Deleting VPC Tags

Function

This API is used to add multiple tags to or delete multiple tags from a VPC at a time.

This API is idempotent.

If there are duplicate keys in the request body when you add tags, an error is reported.

During tag creation, duplicate keys are not allowed. If a key already exists in the database, its value will be overwritten by the new duplicate key.

During tag deletion, if some tags do not exist, the operation is considered to be successful by default. The character set of the tags will not be checked. When you delete tags, the tag structure cannot be missing, and the key cannot be left blank or be an empty string.

URI

POST /v2.0/{project_id}/vpcs/{vpc_id}/tags/action

Table 4-219 describes the parameters.

Table 4-219 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	Specifies the VPC ID, which uniquely identifies the VPC.

Request Parameters

Table 4-220 Request parameter

Parameter	Type	Mandatory	Description
tags	Array of **tag** objects	Yes	Specifies the **tag** objects. For details, see **Table 4-221**.

Parameter	Type	Mandatory	Description
action	String	Yes	Specifies the operation. Possible values are as follows: • **create** • **delete**

Table 4-221 tag objects

Attribute	Type	Mandatory	Description
key	String	Yes	• Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-). • The tag key of a VPC must be unique.
value	String	Yes	• Specifies the tag value. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Request

- Batch create two tags for a VPC.

```
POST https://{Endpoint}/v2.0/{project_id}/vpcs/{vpc_id}/tags/action

{
   "action": "create",
   "tags": [
      {
         "key": "key1",
         "value": "value1"
      },
      {
         "key": "key2",
         "value": "value3"
      }
   ]
}
```

- Batch delete two tags for a VPC.

```
POST https://{Endpoint}/v2.0/{project_id}/vpcs/{vpc_id}/tags/action

{
   "action": "delete",
   "tags": [
```



```
    {
        "key": "key1",
        "value": "value1"
    },
    {
        "key": "key2",
        "value": "value3"
    }
  ]
}
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.10.5 Querying VPCs by Tag

Function

This API is used to query VPCs by tag.

URI

POST /v2.0/{project_id}/vpcs/resource_instances/action

Table 4-222 describes the parameters.

Table 4-222 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-223 Request parameter

Parameter	Type	Mandatory	Description
tags	Array of **tag** objects	No	Specifies the included tags. A maximum of 10 tag keys are allowed for each query operation. Each tag key can have up to 10 tag values. The structure body must be included. The tag key cannot be left blank or set to an empty string. Each tag key must be unique, and each tag value in a tag must be unique.
limit	Integer	No	Sets the page size. This parameter is not available when **action** is set to **count**. The default value is **1000** when **action** is set to **filter**. The maximum value is **1000**, and the minimum value is **1**. The value cannot be a negative number.
offset	Integer	No	Specifies the index position. The query starts from the next piece of data indexed by this parameter. This parameter is not required when you query data on the first page. The value in the response returned for querying data on the previous page will be included in this parameter for querying data on subsequent pages. This parameter is not available when **action** is set to **count**. If **action** is set to **filter**, the value must be a number, and the default value is **0**. The value cannot be a negative number.
action	String	Yes	Specifies the operation to perform. The value can only be **filter** (filtering) or **count** (querying the total number). The value **filter** indicates pagination query. The value **count** indicates that the total number of query results meeting the search criteria will be returned.
matches	Array of **match** objects	No	Specifies the search criteria. The tag key is the field to match. Currently, only **resource_name** is supported. The tag value indicates the matched value. This field is a fixed dictionary value.

Table 4-224 Description of the **tag** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The value can contain a maximum of 128 Unicode characters. The tag key cannot be left blank. (This parameter is not verified during the search process.)
values	Yes	Array of strings	Specifies the tag values. Each value can contain a maximum of 255 Unicode characters. An empty list for **values** indicates any value. The values are in the OR relationship. Resources that match any value can be found. For example, if resource A has a tag value of **val1** and resource B has a tag value of **val2**, resources A and B can be found by using **values={val1,val2}**.

Table 4-225 Description of the **match** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. Currently, the tag key can only be the resource name.
value	Yes	String	Specifies the tag value. Each value can contain a maximum of 255 Unicode characters.

Example Request

- Filter VPCs by setting **action** to **filter**. The query starts from the first record. A maximum of 100 records can be returned for each query. You can use **matches** and **tags** to filter VPCs.

```
POST https://{Endpoint}/v2.0/{project_id}/vpcs/resource_instances/action

{
   "offset": "0",
   "limit": "100",
```



```
  "action": "filter",
  "matches": [
    {
      "key": "resource_name",
      "value": "resource1"
    }
  ],
  "tags": [
    {
      "key": "key1",
      "values": [
        "value1",
        "value2"
      ]
    }
  ]
}
```

- Count VPCs by setting **action** to **count**. Use **matches** and **tags** to filter and count VPCs.

```
POST https://{Endpoint}/v2.0/{project_id}/vpcs/resource_instances/action

{
  "action": "count",
  "tags": [
    {
      "key": "key1",
      "values": [
        "value1",
        "value2"
      ]
    },
    {
      "key": "key2",
      "values": [
        "value1",
        "value2"
      ]
    }
  ],
  "matches": [
    {
      "key": "resource_name",
      "value": "resource1"
    }
  ]
}
```

Response Parameters

Table 4-226 Response parameter

Parameter	Type	Description
resources	Array of **resource** objects	Specifies the **resource** object list. For details, see **Table 4-227**.
total_count	Integer	Specifies the total number of query records.

Table 4-227 resource objects

Parameter	Type	Description
resource_id	String	Specifies the resource ID.
resource_detail	Object	Specifies the resource details. Resource details are used for extension. This parameter is left blank by default.
tags	Array of **tag** objects	Specifies the tag list. This parameter is an empty array by default if there is no tag. For details, see **Table 4-228**.
resource_name	String	Specifies the resource name. This parameter is an empty string by default if there is no resource name.

Table 4-228 Description of the **tag** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The value can contain a maximum of 128 Unicode characters. The tag key cannot be left blank. (This parameter is not verified during the search process.)
value	Yes	String	Specifies the tag value list. Each value can contain a maximum of 255 Unicode characters. An empty list for **values** indicates any value. The values are in the OR relationship. Resources that match any value can be found. For example, if resource A has a tag value of **val1** and resource B has a tag value of **val2**, resources A and B can be found by using **values={val1,val2}**.

Example Response

- When **action** is set to **filter**:

```
{
    "resources": [
      {
        "resource_detail": null,
        "resource_id": "cdfs_cefs_wesas_12_dsad",
        "resource_name": "resouece1",
        "tags": [
          {
            "key": "key1",
            "value": "value1"
          },
          {
            "key": "key2",
            "value": "value1"
          }
        ]
      }
    ],
    "total_count": 1000
}
```

- When **action** is set to **count**:

```
{
     "total_count": 1000
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.10.6 Querying VPC Tags in a Specified Project

Function

This API is used to query all VPC tags of a tenant in a specified region.

URI

GET /v2.0/{project_id}/vpcs/tags

Table 4-229 describes the parameters.

Table 4-229 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/{project_id}/vpcs/tags
```

Response Parameters

Table 4-230 Response parameter

Parameter	Type	Description
tags	Array of **tag** objects	Specifies the tag list.

Table 4-231 Description of the **tag** field

Parameter	Type	Description
key	String	Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-).
values	Array of strings	Specifies the tag value list. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Response

```
{
  "tags": [
    {
      "key": "key1",
      "values": [
        "value1",
        "value2"
      ]
    },
    {
      "key": "key2",
      "values": [
        "value1",
        "value2"
      ]
```



```
    }
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.11 Subnet Tag Management

4.11.1 Adding a Tag to a Subnet

Function

This API is used to add a tag to a subnet.

URI

POST /v2.0/{project_id}/subnets/{subnet_id}/tags

Table 4-232 describes the parameters.

Table 4-232 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
subnet_id	Yes	Specifies the subnet ID, which uniquely identifies the subnet. If you use the management console, the value of this parameter is the **Network ID** value.

Request Parameters

Table 4-233 Request parameter

Parameter	Type	Mandatory	Description
tag	**tag** object	Yes	Specifies the **tag** objects. For details, see **Table 4-234**.

Table 4-234 tag objects

Attribute	Type	Mandatory	Description
key	String	Yes	• Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-). • The tag key of a VPC must be unique.
value	String	Yes	• Specifies the tag value. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Request

- Create a tag for a subnet. The key is **key1**, and the value is **value1**.

```
POST https://{Endpoint}/v2.0/{project_id}/subnets/{subnet_id}/tags

{
   "tag": {
      "key": "key1",
      "value": "value1"
   }
}
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.11.2 Querying Subnet Tags

Function

This API is used to query tags of a specified subnet.

URI

GET /v2.0/{project_id}/subnets/{subnet_id}/tags

Table 4-235 describes the parameters.

Table 4-235 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
subnet_id	Yes	Specifies the subnet ID that uniquely identifies the subnet. If you use the management console, the value of this parameter is the **Network ID** value.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/{project_id}/subnets/{subnet_id}/tags
```


Response Parameters

Table 4-236 Response parameter

Parameter	Type	Description
tags	Array of **tag** objects	Specifies the **tag** object list. For details, see **Table 4-237**.

Table 4-237 tag objects

Attribute	Type	Description
key	String	• Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-). • The tag key of a VPC must be unique.
value	String	• Specifies the tag value. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Response

```
{
   "tags": [
      {
         "key": "key1",
         "value": "value1"
      },
      {
         "key": "key2",
         "value": "value3"
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.11.3 Deleting a Tag from a Subnet

Function

This API is used to delete a tag from subnet.

URI

DELETE /v2.0/{project_id}/subnets/{subnet_id}/tags/{key}

Table 4-238 describes the parameters.

Table 4-238 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
subnet_id	Yes	Specifies the subnet ID, which uniquely identifies the subnet. If you use the management console, the value of this parameter is the **Network ID** value.
key	Yes	Specifies the tag key.

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/{project_id}/subnets/{subnet_id}/tags/{key}
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.11.4 Batch Adding or Deleting Subnet Tags

Function

This API is used to add multiple tags to or delete multiple tags from a subnet at a time.

This API is idempotent.

If there are duplicate keys in the request body when you add tags, an error is reported.

During tag creation, duplicate keys are not allowed. If a key already exists in the database, its value will be overwritten by the new duplicate key.

During tag deletion, if some tags do not exist, the deletion is considered to be successful by default. The character set of the tags will not be checked. When you delete tags, the tag structure cannot be missing, and the key cannot be left blank or be an empty string.

URI

POST /v2.0/{project_id}/subnets/{subnet_id}/tags/action

Table 4-239 describes the parameters.

Table 4-239 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
subnet_id	Yes	Specifies the subnet ID, which uniquely identifies the subnet. If you use the management console, the value of this parameter is the **Network ID** value.

Request Parameters

Table 4-240 Request parameter

Parameter	Type	Mandatory	Description
tags	Array of **tag** objects	Yes	Specifies the **tag** object list. For details, see **Table 4-241**.
action	String	Yes	Specifies the operation. Possible values are as follows: • **create** • **delete**

Table 4-241 tag objects

Attribute	Type	Mandatory	Description
key	String	Yes	• Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-). • The tag key of a VPC must be unique.
value	String	Yes	• Specifies the tag value. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Request

- Batch create two tags for a subnet.

```
POST https://{Endpoint}/v2.0/{project_id}/subnets/{subnet_id}/tags/action

{
   "action": "create",
   "tags": [
      {
         "key": "key1",
         "value": "value1"
      },
      {
         "key": "key2",
```



```
            "value": "value3"
        }
    ]
}
```

- Batch delete two tags for a subnet.

```
POST https://{Endpoint}/v2.0/{project_id}/subnets/{subnet_id}/tags/action

{
    "action": "delete",
    "tags": [
        {
            "key": "key1",
            "value": "value1"
        },
        {
            "key": "key2",
            "value": "value3"
        }
    ]
}
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.11.5 Querying Subnets by Tag

Function

This API is used to query subnets by tag.

URI

POST /v2.0/{project_id}/subnets/resource_instances/action

Table 4-242 describes the parameters.

Table 4-242 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-243 Request parameter

Parameter	Type	Mandatory	Description
tags	Array of **tag** objects	No	Specifies the included tags. A maximum of 10 tag keys are allowed for each query operation. Each tag key can have up to 10 tag values. The structure body must be included. The tag key cannot be left blank or set to an empty string. Each tag key must be unique, and each tag value in a tag must be unique.
limit	Integer	No	Sets the page size. This parameter is not available when **action** is set to **count**. The default value is **1000** when **action** is set to **filter**. The maximum value is **1000**, and the minimum value is **1**. The value cannot be a negative number.
offset	Integer	No	Specifies the index position. The query starts from the next piece of data indexed by this parameter. This parameter is not required when you query data on the first page. The value in the response returned for querying data on the previous page will be included in this parameter for querying data on subsequent pages. This parameter is not available when **action** is set to **count**. If **action** is set to **filter**, the value must be a number, and the default value is **0**. The value cannot be a negative number.
action	String	Yes	Specifies the operation to perform. The value can only be **filter** (filtering) or **count** (querying the total number). The value **filter** indicates pagination query. The value **count** indicates that the total number of query results meeting the search criteria will be returned.
matches	Array of **match** objects	No	Specifies the search criteria. The tag key is the field to match. Currently, only **resource_name** is supported. The tag value indicates the matched value. This field is a fixed dictionary value.

Table 4-244 Description of the **tag** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The value can contain a maximum of 128 Unicode characters. The tag key cannot be left blank. (This parameter is not verified during the search process.)
values	Yes	Array of strings	Specifies the tag value list. Each value can contain a maximum of 255 Unicode characters. An empty list for **values** indicates any value. The values are in the OR relationship.

Table 4-245 Description of the **match** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. Currently, the tag key can only be the resource name.
value	Yes	String	Specifies the tag value. Each value can contain a maximum of 255 Unicode characters.

Example Request

- Filter subnets by setting **action** to **filter**. The query starts from the first record. A maximum of 100 records can be returned for each query. You can use **matches** and **tags** to filter subnets.

```
POST https://{Endpoint}/v2.0/{project_id}/subnets/resource_instances/action

{
   "offset": "0",
   "limit": "100",
   "action": "filter",
   "matches": [
      {
         "key": "resource_name",
         "value": "resource1"
      }
   ],
   "tags": [
      {
         "key": "key1",
         "values": [
```



```
            "value1",
            "value2"
        ]
    }
  ]
}
```

- Count subnets by setting **action** to **count**. Use **matches** and **tags** to filter and count VPCs.

```
POST https://{Endpoint}/v2.0/{project_id}/subnets/resource_instances/action

{
  "action": "count",
  "tags": [
    {
      "key": "key1",
      "values": [
        "value1",
        "value2"
      ]
    },
    {
      "key": "key2",
      "values": [
        "value1",
        "value2"
      ]
    }
  ],
  "matches": [
    {
      "key": "resource_name",
      "value": "resource1"
    }
  ]
}
```

Response Parameters

Table 4-246 Response parameter

Parameter	Type	Description
resources	Array of **resource** objects	Specifies the **resource** object list. For details, see **Table 4-247**.
total_count	Integer	Specifies the total number of query records.

Table 4-247 resource objects

Parameter	Type	Description
resource_id	String	Specifies the resource ID.

Parameter	Type	Description
resource_detail	Object	Specifies the resource details. Resource details are used for extension. This parameter is left blank by default.
tags	Array of **tag** objects	Specifies the tag list. This parameter is an empty array by default if there is no tag. For details, see **Table 4-248**.
resource_name	String	Specifies the resource name. This parameter is an empty string by default if there is no resource name.

Table 4-248 Description of the **tag** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The value can contain a maximum of 128 Unicode characters. The tag key cannot be left blank. (This parameter is not verified during the search process.)
value	Yes	String	Specifies the tag value list. Each value can contain a maximum of 255 Unicode characters. An empty list for **values** indicates any value. The values are in the OR relationship.

Example Response

- When **action** is set to **filter**:

```
{
    "resources": [
      {
        "resource_detail": null,
        "resource_id": "cdfs_cefs_wesas_12_dsad",
        "resource_name": "resouece1",
        "tags": [
          {
            "key": "key1",
```

```
            "value": "value1"
          },
          {
            "key": "key2",
            "value": "value1"
          }
        ]
      }
    ],
    "total_count": 1000
}
```

- When **action** is set to **count**:

```
{
    "total_count": 1000
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.11.6 Querying Subnet Tags in a Specified Project

Function

This API is used to query all subnet tags of a tenant in a specified region.

URI

GET /v2.0/{project_id}/subnets/tags

Table 4-249 describes the parameters.

Table 4-249 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/{project_id}/subnets/tags
```


Response Parameters

Table 4-250 Response parameter

Parameter	Type	Description
tags	Array of **tag** objects	Specifies the **tag** object list. For details, see **Table 4-251**.

Table 4-251 Description of the **tag** field

Parameter	Type	Description
key	String	Specifies the tag key. • Cannot be left blank. • Contain up to 128 characters (36 characters on the console). • Can contain letters, digits, underscores (_), and hyphens (-).
values	Array of strings	Specifies the tag value list. • Contain up to 255 characters (43 characters on the console). • Can contain letters, digits, underscores (_), periods (.), and hyphens (-).

Example Response

```
{
  "tags": [
    {
      "key": "key1",
      "values": [
        "value1",
        "value2"
      ]
    },
    {
      "key": "key2",
      "values": [
        "value1",
        "value2"
      ]
    }
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.12 Security Group Tag Management

4.12.1 Querying Security Groups by Tag

Function

This API is used to query security group by tag.

URI

POST /v2.0/{project_id}/security-groups/resource_instances/action

Table 4-252 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-253 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Operation The value can be filter or count.
limit	No	Integer	Number of records to be queried. Value range: 1 to 1000 This parameter is not available when action is set to count. The default value is 1000 when action is set to filter.

Parameter	Mandatory	Type	Description
offset	No	Integer	Index position. The query starts from the next data record indexed by this parameter. You do not need to specify this parameter when you query resources on the first page. When you query resources on subsequent pages, set this parameter to the location returned in the response body for the previous query. This parameter is not available when action is set to count. If action is set to filter, the value must be a number, and the default value is 0. The value cannot be a negative number.
matches	No	Array of **Match** objects	Search criteria. The tag key is the field to match, and the tag value indicates the matched value. Currently, only resource_name is supported.
tags	No	Array of **ListTag** objects	Included tags. Each tag contains a maximum of 10 keys, and each key contains a maximum of 10 values. The structure body cannot be missing, and the key cannot be left blank or set to an empty string. Each tag key must be unique, and each tag value in a tag must be unique.

Table 4-254 Match

Parameter	Mandatory	Type	Description
key	Yes	String	Key. The tag key can only be the resource name.

Parameter	Mandatory	Type	Description
value	Yes	String	Value. Each value can contain a maximum of 255 Unicode characters and cannot contain special characters, such as dollar signs ($), hyphens (-), periods (.), or slashes (/). Maximum: **255**

Table 4-255 ListTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key cannot be left blank. Minimum: **1** Maximum: **127**
values	Yes	Array of strings	Tag values. If values are null, it indicates any_value. All values of a tag key are in the OR relationship.

Response Parameters

Status code: 200

Table 4-256 Response body parameters

Parameter	Type	Description
resources	Array of **ListResourceResp** objects	Resources
total_count	Integer	Number of resources.

Table 4-257 ListResourceResp

Parameter	Type	Description
resource_detail	Object	Resource details used for extension, which is left blank by default.
resource_id	String	Resource ID

Parameter	Type	Description
resource_name	String	Resource name. If there is no resource name, this parameter is an empty string by default.
tags	Array of ResourceTag objects	A list of tags. This parameter is an empty array by default if there is no tag.

Table 4-258 ResourceTag

Parameter	Type	Description
key	String	Tag key. The key must be unique for each resource. Minimum: **0** Maximum: **36**
value	String	Tag value Minimum: **0** Maximum: **43**

Status code: 400

Table 4-259 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 401

Table 4-260 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 403

Table 4-261 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 404

Table 4-262 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 409

Table 4-263 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 500

Table 4-264 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Example Requests

- example-1: Request body when action is set to filter

```
POST https://{Endpoint}/v2.0/{project_id}/security-groups/resource_instances/action

{
  "offset" : "0",
  "limit" : "100",
  "action" : "filter",
  "matches" : [ {
    "key" : "resource_name",
    "value" : "resource1"
```

```
 } ],
 "tags" : [ {
   "key" : "key1",
   "values" : [ "*value1", "value2" ]
 } ]
}
```

- example-2: Request body when action is set to count

```
POST https://{Endpoint}/v2.0/{project_id}/security-groups/resource_instances/action

{
 "action" : "count",
 "tags" : [ {
   "key" : "key1",
   "values" : [ "value1", "value2" ]
 }, {
   "key" : "key2",
   "values" : [ "value1", "value2" ]
 } ],
 "matches" : [ {
   "key" : "resource_name",
   "value" : "resource1"
 } ]
}
```

Example Responses

Status code: 200

If action in the request body is set to filter, the resource tag list is returned. If action in the request body is set to count, the total number of tags is returned.

```
{
  "resources" : [ {
    "resource_id" : "cdfs_cefs_wesas_12_dsad",
    "resource_name" : "resouece1",
    "tags" : [ {
      "key" : "key1",
      "value" : "value1"
    }, {
      "key" : "key2",
      "value" : "value1"
    } ]
  } ],
  "total_count" : 1000
}
```

Status Codes

Status Code	Description
200	If action in the request body is set to filter, the resource tag list is returned. If action in the request body is set to count, the total number of tags is returned.
400	The server failed to process the request.
401	Username and password are required to access the page requested.
403	You are forbidden to access the requested page.
404	The server could not find the requested page.

Status Code	Description
409	The request could not be processed due to a conflict.
500	Failed to complete the request because of an internal service error.

Error Codes

See **Error Codes**.

4.12.2 Batch Adding Tags to a Security Group

Function

This API is used to add multiple tags to a security group at a time.

The API is idempotent. When you create tags, if there are duplicate keys in the request body, an error is reported. During tag creation, duplicate keys are not allowed. If a key already exists in the database, its value will be overwritten by the new duplicate key.

Constraints

The API is idempotent. When you create tags, if there are duplicate keys in the request body, an error is reported. During tag creation, duplicate keys are not allowed. If a key already exists in the database, its value will be overwritten by the new duplicate key.

URI

POST /v2.0/{project_id}/security-groups/{security_group_id}/tags/action

Table 4-265 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
security_group_id	Yes	String	Security Group ID

Request Parameters

Table 4-266 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Operation

Parameter	Mandatory	Type	Description
tags	Yes	Array of ResourceTag objects	Tag list

Table 4-267 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key must be unique for each resource. Minimum: **0** Maximum: **36**
value	Yes	String	Tag value Minimum: **0** Maximum: **43**

Response Parameters

Status code: 400

Table 4-268 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 401

Table 4-269 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 403

Table 4-270 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 404

Table 4-271 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 409

Table 4-272 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 500

Table 4-273 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Example Requests

- example-1: Deleting a tag

```
POST https://{Endpoint}/v2.0/{project_id}/security-groups/{security_group_id}/tags/action

{
  "action" : "delete",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
```

```
    "value" : "value3"
  } ]
}
```

- example-2: Creating a tag

```
POST https://{Endpoint}/v2.0/{project_id}/security-groups/{security_group_id}/tags/action

{
  "action" : "create",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value3"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
204	Normal response.
400	The server failed to process the request.
401	Username and password are required to access the page requested.
403	You are forbidden to access the requested page.
404	The server could not find the requested page.
409	The request could not be processed due to a conflict.
500	Failed to complete the request because of an internal service error.

Error Codes

See **Error Codes**.

4.12.3 Batch Deleting Tags from a Security Group

Function

This API is used to delete multiple tags from a security group at a time.

This API is idempotent. During tag deletion, if some tags do not exist, the deletion is considered to be successful by default. The character set of the tags will not be checked. When you delete tags, the tag structure cannot be missing, and the key cannot be left blank or be an empty string.

URI

POST /v2.0/{project_id}/security-groups/{security_group_id}/tags/action

Table 4-274 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
security_group_id	Yes	String	Security Group ID

Request Parameters

Table 4-275 Request body parameters

Parameter	Mandatory	Type	Description
action	Yes	String	Operation
tags	Yes	Array of **ResourceTag** objects	Tag list

Table 4-276 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key must be unique for each resource. Minimum: **0** Maximum: **36**
value	Yes	String	Tag value Minimum: **0** Maximum: **43**

Response Parameters

Status code: 400

Table 4-277 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 401

Table 4-278 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 403

Table 4-279 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 404

Table 4-280 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 409

Table 4-281 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 500

Table 4-282 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Example Requests

- example-1: Creating a tag

```
POST https://{Endpoint}/v2.0/{project_id}/security-groups/{security_group_id}/tags/action

{
  "action" : "create",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value3"
  } ]
}
```

- example-2: Deleting a tag

```
POST https://{Endpoint}/v2.0/{project_id}/security-groups/{security_group_id}/tags/action

{
  "action" : "delete",
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value3"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
204	Normal response.
400	The server failed to process the request.
401	Username and password are required to access the page requested.
403	You are forbidden to access the requested page.
404	The server could not find the requested page.

Status Code	Description
409	The request could not be processed due to a conflict.
500	Failed to complete the request because of an internal service error.

Error Codes

See **Error Codes**.

4.12.4 Querying Security Group Tags

Function

This API is used to query tags of a specified security group.

URI

GET /v2.0/{project_id}/security-groups/{security_group_id}/tags

Table 4-283 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
security_group_id	Yes	String	Security Group ID

Request Parameters

None

Response Parameters

Status code: 200

Table 4-284 Response body parameters

Parameter	Type	Description
tags	Array of **ResourceTag** objects	Tags

Table 4-285 ResourceTag

Parameter	Type	Description
key	String	Tag key. The key must be unique for each resource. Minimum: **0** Maximum: **36**
value	String	Tag value Minimum: **0** Maximum: **43**

Status code: 400

Table 4-286 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 401

Table 4-287 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 403

Table 4-288 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 404

Table 4-289 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 409

Table 4-290 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 500

Table 4-291 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Example Requests

Querying Security Group Tags

```
GET https://{Endpoint}/v2.0/{project_id}/security-groups/{security_group_id}/tags
```

Example Responses

Status code: 200

Normal response.

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value3"
  } ]
}
```


Status Codes

Status Code	Description
200	Normal response.
400	The server failed to process the request.
401	Username and password are required to access the page requested.
403	You are forbidden to access the requested page.
404	The server could not find the requested page.
409	The request could not be processed due to a conflict.
500	Failed to complete the request because of an internal service error.

Error Codes

See **Error Codes**.

4.12.5 Adding a Tag to a Security Group

Function

This API is used to create a tag for a security group.The API is idempotent. If a to-be-created tag has the same key as an existing tag, the tag will be created and overwrite the existing one.

URI

POST /v2.0/{project_id}/security-groups/{security_group_id}/tags

Table 4-292 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
security_group_id	Yes	String	Security Group ID

Request Parameters

Table 4-293 Request body parameters

Parameter	Mandatory	Type	Description
tag	Yes	ResourceTag object	Request body for creating a security group tag.

Table 4-294 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key must be unique for each resource. Minimum: **0** Maximum: **36**
value	Yes	String	Tag value Minimum: **0** Maximum: **43**

Response Parameters

Status code: 400

Table 4-295 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 401

Table 4-296 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 403

Table 4-297 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 404

Table 4-298 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 409

Table 4-299 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 500

Table 4-300 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Example Requests

Creating a Tag for a Security Group

```
POST https://{Endpoint}/v2.0/{project_id}/security-groups/{security_group_id}/tags

{
  "tag" : {
    "key" : "key1",
    "value" : "value1"
  }
}
```


Example Responses

None

Status Codes

Status Code	Description
204	Normal response.
400	The server failed to process the request.
401	Username and password are required to access the page requested.
403	You are forbidden to access the requested page.
404	The server could not find the requested page.
409	The request could not be processed due to a conflict.
500	Failed to complete the request because of an internal service error.

Error Codes

See **Error Codes**.

4.12.6 Deleting a Tag from a Security Group

Function

This API is used to delete a security group tag.This API is idempotent. If the key to be deleted does not exist, error 404 is reported. The key cannot be empty or an empty string.

URI

DELETE /v2.0/{project_id}/security-groups/{security_group_id}/tags/{key}

Table 4-301 Path Parameters

Parameter	Mandatory	Type	Description
key	Yes	String	Key value
project_id	Yes	String	Project ID
security_group_id	Yes	String	Security Group ID

Request Parameters

None

Response Parameters

Status code: 400

Table 4-302 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 401

Table 4-303 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 403

Table 4-304 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 404

Table 4-305 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 409

Table 4-306 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 500

Table 4-307 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Example Requests

Deleting a Security Group Tag

```
DELETE https://{Endpoint}/v2.0/{project_id}/security-groups/{security_group_id}/tags/{key}
```

Example Responses

None

Status Codes

Status Code	Description
204	Normal response.
400	The server failed to process the request.
401	Username and password are required to access the page requested.
403	You are forbidden to access the requested page.
404	The server could not find the requested page.
409	The request could not be processed due to a conflict.
500	Failed to complete the request because of an internal service error.

Error Codes

See **Error Codes**.

4.12.7 Querying Security Group Tags in a Specified Project

Function

This API is used to query all security group tags of a tenant in a specified region.

URI

GET /v2.0/{project_id}/security-groups/tags

Table 4-308 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

None

Response Parameters

Status code: 200

Table 4-309 Response body parameters

Parameter	Type	Description
tags	Array of **ListTag** objects	Tags

Table 4-310 ListTag

Parameter	Type	Description
key	String	Tag key. The key cannot be left blank. Minimum: **1** Maximum: **127**
values	Array of strings	Tag values. If values are null, it indicates any_value. All values of a tag key are in the OR relationship.

Status code: 400

Table 4-311 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 401

Table 4-312 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 403

Table 4-313 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 404

Table 4-314 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 409

Table 4-315 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Status code: 500

Table 4-316 Response body parameters

Parameter	Type	Description
code	String	Error code returned for a request.
message	String	Error message returned for a request.

Example Requests

Querying Security Group Tags in a Specified Project

```
GET https://{Endpoint}/v2.0/{project_id}/security-groups/tags
```

Example Responses

Status code: 200

Normal response.

```
{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  }, {
    "key" : "key2",
    "values" : [ "value1", "value2" ]
  } ]
}
```

Status Codes

Status Code	Description
200	Normal response.
400	The server failed to process the request.
401	Username and password are required to access the page requested.
403	You are forbidden to access the requested page.
404	The server could not find the requested page.
409	The request could not be processed due to a conflict.
500	Failed to complete the request because of an internal service error.

Error Codes

See **Error Codes**.

4.13 Querying IP Address Usage

4.13.1 Querying IP Address Usage on a Specified Network

Function

This API is used to query the IP address usage on a specified network.

The obtained information includes the total number of IP addresses on the network, the number of in-use IP addresses on the network, the total number of IP addresses on each subnet, and the number of in-use IP addresses on the subnet.

NOTICE

- The first and the last two IP addresses on each subnet are reserved by the system for the gateway and DHCP service.
- The total number of IP addresses and the number of in-use IP addresses described in this section and the subsequent sections do not include the IP addresses reserved by the system.
- When assigning an IP address, you can specify the reserved IP address for the system. The reserved IP addresses will not be included in the number of in-use IP addresses and the total number of IP addresses no matter how the IP address is assigned.

URI

GET /v2.0/network-ip-availabilities/{network_id}

Table 4-317 describes the parameters.

Table 4-317 Parameter description

Parameter	Type	Mandatory	Description
network_id	String	Yes	Specifies the network ID. **NOTE** **network_id** indicates the subnet ID used when the VPC subnet API is called. For more information, see **What Is the Difference Between the VPC Subnet API and the OpenStack Neutron Subnet API?**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/network-ip-availabilities/6b50d967-779c-40c9-a157-de1df3c17043
```

Response Parameters

Table 4-318 Response parameter

Parameter	Type	Description
network_ip_availability	**network_ip_availability** object	Specifies the **network_ip_availability** objects. For details, see **Table 4-319**.

Table 4-319 network_ip_availability objects

Parameter	Type	Description
network_id	String	Specifies the network ID.
network_name	String	Specifies the network name.
tenant_id	String	Specifies the project ID.
total_ips	Integer	Specifies the total number of IP addresses on a network. (System reserved IP addresses are not included.)
used_ips	Integer	Specifies the number of in-use IP addresses on a network. (Reserved IP addresses are not included.)
subnet_ip_availability	Array of **subnet_ip_availability** objects	Specifies the subnet IP address usage objects. For details, see **Table 4-320**.

Table 4-320 Description of the **subnet_ip_availability** field

Parameter	Type	Description
used_ips	Integer	Specifies the number of in-use IP addresses on a subnet. (System reserved IP addresses are not included.)
subnet_id	String	Specifies the subnet ID. If you use the management console, the value of this parameter is the **Network ID** value.
subnet_name	String	Specifies the subnet name.
ip_version	Integer	Specifies the IP version of the subnet. Only IPv4 is supported.
cidr	String	Specifies the subnet CIDR block.
total_ips	Integer	Specifies the total number of IP addresses on a subnet. (System reserved IP addresses are not included.)

Example Response

```
{
  "network_ip_availability": {
    "used_ips": 4,
    "subnet_ip_availability": [
      {
        "used_ips": 4,
        "subnet_id": "98e343d1-3cb8-4f69-9cd1-00569819480f",
        "subnet_name": "",
        "ip_version": 4,
        "cidr": "10.0.0.0/8",
        "total_ips": 300
      }
    ],
    "network_id": "6b50d967-779c-40c9-a157-de1df3c17043",
    "tenant_id": "7c4b23cb125d481c95cbe4f91b2c11cd",
    "total_ips": 300,
    "network_name": "pch_test_003"
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.14 VPC Flow Log

4.14.1 Creating a VPC Flow Log

Function

This API is used to create a VPC flow log.

A VPC flow log captures information about the traffic going to and from your VPC. You can use flow logs to monitor network traffic, analyze network attacks, and to determine whether security group and network ACL rules need to be modified.

VPC flow logs must be used together with the Log Tank Service (LTS). You need to create a log group and a log topic in LTS, and then create a VPC flow log.

NOTE

The VPC flow log function is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, LA-Mexico City2, and AF-Johannesburg.

URI

POST /v1/{project_id}/fl/flow_logs

Table 4-321 describes the parameters.

Table 4-321 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameters

Table 4-322 Request parameter

Parameter	Mandatory	Type	Description
flow_log	Yes	**flow_log** object	**FlowLog** objects. For details, see **Table 4-323**.

Table 4-323 Description of the **FlowLog** field

Parameter	Mandatory	Type	Description
name	No	String	• Flow log name. • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	• Flow log description • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
resource_type	Yes	String	• Type of the resource for which that the logs to be collected. • The value can be: – **port**: NIC – **vpc**: All NICs in a VPC – **network**: All NICs in a subnet
resource_id	Yes	String	• ID of the resource for which that the logs to be collected.
traffic_type	Yes	String	• Type of the traffic for which that the logs to be collected. • The value can be: – **all**: specifies that both accepted and rejected traffic of the specified resource will be logged. – **accept**: specifies that only accepted inbound and outbound traffic of the specified resource will be logged. – **reject**: specifies that only rejected inbound and outbound traffic of the specified resource will be logged.
log_group_id	Yes	String	• Log group ID
log_topic_id	Yes	String	• Log topic ID

Example Request

- Create a VPC flow log. Set the resource type to port, resource ID to 05c4052d-8d14-488f-aa00-19fea5a25fde, traffic type to reject, log group ID to

05c4052d-8d14-488f-aa00-19fea5a25fdd, and log topic ID to a9d7dee7-37d2-4cba-a208-a016252aaa63.

```
POST https://{Endpoint}/v1/b2782e6708b8475c993e6064bc456bf8/fl/flow_logs

{
   "flow_log": {
      "name": "flowlog",
      "description": "just a test",
      "resource_type": "port",
      "resource_id": "05c4052d-8d14-488f-aa00-19fea5a25fde",
      "traffic_type": "reject",
      "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fdd",
      "log_topic_id": "a9d7dee7-37d2-4cba-a208-a016252aaa63"
   }
}
```

Response Parameters

Table 4-324 Response parameter

Parameter	Type	Description
flow_log	**flow_log** object	**FlowLog** objects. For details, see **Table 4-325**.

Table 4-325 Description of the **FlowLog** field

Parameter	Type	Description
id	String	• Flow log ID
name	String	• Flow log name • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
tenant_id	String	• Project ID
description	String	• Flow log description • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
resource_type	String	• Type of the resource for which that the logs to be collected. • The value can be: – **port**: NIC – **vpc**: All NICs in a VPC – **network**: All NICs in a subnet
resource_id	String	• ID of the resource for which that the logs to be collected.

Parameter	Type	Description
traffic_type	String	• Type of the traffic for which that the logs to be collected. • The value can be: – **all**: specifies that both accepted and rejected traffic of the specified resource will be logged. – **accept**: specifies that only accepted inbound and outbound traffic of the specified resource will be logged. – **reject**: specifies that only rejected inbound and outbound traffic of the specified resource will be logged.
log_group_id	String	• Log group ID
log_topic_id	String	• Log topic ID
log_store_type	String	• Service that is used to store flow logs • The value can be: – **lts**: Log Tank Service (LTS)
admin_state	Boolean	• Whether to enable the flow log function
status	String	• Flow log status • The value can be: – **ACTIVE**: Enabled – **DOWN**: Disabled – **ERROR**: Abnormal
created_at	String	• Time when the flow log is created • UTC time in the format of yyyy-MM-ddTHH:mmss
updated_at	String	• Time when the flow log is updated • UTC time in the format of yyyy-MM-ddTHH:mmss

Example Response

```
{
   "flow_log": {
      "id": "f49f00f1-0f15-470a-a8c5-4e879e461c8d",
      "name": "flowlog",
      "description": "just a test",
      "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
      "resource_type": "port",
      "resource_id": "05c4052d-8d14-488f-aa00-19fea5a25fde",
      "traffic_type": "reject",
      "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fdd",
      "log_topic_id": "a9d7dee7-37d2-4cba-a208-a016252aaa63",
```



```
    "log_store_type": "lts",
    "created_at": "2019-01-14T11:03:02",
    "updated_at": "2019-01-14T11:03:02",
    "admin_state": true,
    "status": "ACTIVE"
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.14.2 Querying VPC Flow Logs

Function

This API is used to query all VPC flow logs of the tenant submitting the request. The VPC flow logs are filtered based on the filtering condition.

URI

GET /v1/{project_id}/fl/flow_logs

Example:

```
GET https://{Endpoint}/v1/b2782e6708b8475c993e6064bc456bf8/fl/flow_logs?name=flowlog
```

Table 4-326 describes the parameters.

Table 4-326 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	• Project ID. For details, see **Obtaining a Project ID**.
id	No	String	• Flow log ID
name	No	String	• Flow log name • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
tenant_id	No	String	• Project ID

Parameter	Mandatory	Type	Description
description	No	String	• Flow log description • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
resource_type	No	String	• Type of the resource for which that the logs to be collected. • The value can be: – **port**: NIC – **vpc**: All NICs in a VPC – **network**: All NICs in a subnet
resource_id	No	String	• ID of the resource for which that the logs to be collected.
traffic_type	No	String	• Type of the traffic for which that the logs to be collected. • The value can be: – **all**: specifies that both accepted and rejected traffic of the specified resource will be logged. – **accept**: specifies that only accepted inbound and outbound traffic of the specified resource will be logged. – **reject**: specifies that only rejected inbound and outbound traffic of the specified resource will be logged.
log_group_id	No	String	• Log group ID
log_topic_id	No	String	• Log topic ID

Parameter	Mandatory	Type	Description
log_store_type	No	String	• Service that is used to store flow logs • The value can be: – **lts**: Log Tank Service (LTS)
status	No	String	Flow log status • **ACTIVE**: Enabled • **DOWN**: Disabled • **ERROR**: Abnormal
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/b2782e6708b8475c993e6064bc456bf8/fl/flow_logs?name=flowlog
```


Response Parameters

Table 4-327 Response parameter

Parameter	Type	Description
flow_logs	Array of **FlowLog** objects	**FlowLog** object list. For details, see **Table 4-328**.

Table 4-328 Description of the **FlowLog** field

Parameter	Type	Description
id	String	• Flow log ID
name	String	• Flow log name • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
tenant_id	String	• Project ID
description	String	• Flow log description • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
resource_type	String	• Type of the resource for which that the logs to be collected. • The value can be: – **port**: NIC – **vpc**: All NICs in a VPC – **network**: All NICs in a subnet
resource_id	String	• ID of the resource for which that the logs to be collected.
traffic_type	String	• Type of the traffic for which that the logs to be collected. • The value can be: – **all**: specifies that both accepted and rejected traffic of the specified resource will be logged. – **accept**: specifies that only accepted inbound and outbound traffic of the specified resource will be logged. – **reject**: specifies that only rejected inbound and outbound traffic of the specified resource will be logged.

Parameter	Type	Description
log_group_id	String	• Log group ID
log_topic_id	String	• Log topic ID
log_store_type	String	• Service that is used to store flow logs • The value can be: – **lts**: Log Tank Service (LTS)
admin_state	Boolean	• Whether to enable the flow log function
status	String	• Flow log status • The value can be: – **ACTIVE**: Enabled – **DOWN**: Disabled – **ERROR**: Abnormal
created_at	String	• Time when the flow log is created • UTC time in the format of yyyy-MM-ddTHH:mmss
updated_at	String	• Time when the flow log is updated • UTC time in the format of yyyy-MM-ddTHH:mmss

Example Response

```
{
   "flow_logs": [
      {
         "id": "35868d55-443e-4d5c-90a4-ac618dc45c1a",
         "name": "flowlog",
         "description": "just a test",
         "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
         "resource_type": "port",
         "resource_id": "05c4052d-8d14-488f-aa00-19fea5a25fde",
         "traffic_type": "reject",
         "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fff",
         "log_topic_id": "a9d7dee7-37d2-4cba-a208-a016252aaa63",
         "log_store_type": "lts",
         "created_at": "2019-01-14T11:03:02",
         "updated_at": "2019-01-14T11:03:02",
         "status": "ACTIVE",
         "admin_state": true
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.14.3 Querying a VPC Flow Log

Function

This API is used to query a VPC flow log.

URI

GET /v1/{project_id}/fl/flow_logs/{flowlog_id}

Table 4-329 describes the parameters.

Table 4-329 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
flowlog_id	Yes	String	Flow log ID

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v1/b2782e6708b8475c993e6064bc456bf8/fl/flow_logs/1e10cd9d-742a-4d36-a9fd-aee9784336ff
```

Response Parameters

Table 4-330 Response parameter

Parameter	Type	Description
flow_log	**flow_log** object	**FlowLog** objects. For details, see **Table 4-331**.

Table 4-331 Description of the **FlowLog** field

Parameter	Type	Description
id	String	• Flow log ID
name	String	• Flow log name • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
tenant_id	String	• Project ID
description	String	• Flow log description • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
resource_type	String	• Type of the resource for which that the logs to be collected. • The value can be: – **port**: NIC – **vpc**: All NICs in a VPC – **network**: All NICs in a subnet
resource_id	String	• ID of the resource for which that the logs to be collected.
traffic_type	String	• Type of the traffic for which that the logs to be collected. • The value can be: – **all**: specifies that both accepted and rejected traffic of the specified resource will be logged. – **accept**: specifies that only accepted inbound and outbound traffic of the specified resource will be logged. – **reject**: specifies that only rejected inbound and outbound traffic of the specified resource will be logged.
log_group_id	String	• Log group ID
log_topic_id	String	• Log topic ID
log_store_type	String	• Service that is used to store flow logs • The value can be: – **lts**: Log Tank Service (LTS)
admin_state	Boolean	• Whether to enable the flow log function

Parameter	Type	Description
status	String	• Flow log status • The value can be: – **ACTIVE**: Enabled – **DOWN**: Disabled – **ERROR**: Abnormal
created_at	String	• Time when the flow log is created • UTC time in the format of yyyy-MM-ddTHH:mmss
updated_at	String	• Time when the flow log is updated • UTC time in the format of yyyy-MM-ddTHH:mmss

Example Response

```
{
   "flow_log": {
      "id": "35868d55-443e-4d5c-90a4-ac618dc45c1a",
      "name": "flow",
      "description": "just a test",
      "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
      "resource_type": "port",
      "resource_id": "05c4052d-8d14-488f-aa00-19fea5a25fde",
      "traffic_type": "reject",
      "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fff",
      "log_topic_id": "a9d7dee7-37d2-4cba-a208-a016252aaa63",
      "log_store_type": "lts",
      "created_at": "2019-01-14T11:03:02",
      "updated_at": "2019-01-14T11:03:02",
      "status": "ACTIVE",
      "admin_state": true
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.14.4 Updating a VPC Flow Log

Function

This API is used to update a VPC flow log.

URI

PUT /v1/{project_id}/fl/flow_logs/{flowlog_id}

Table 4-332 describes the parameters.

Table 4-332 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
flowlog_id	Yes	String	Flow log ID

Request Parameters

Table 4-333 Request parameter

Parameter	Mandatory	Type	Description
flow_log	Yes	**flow_log** object	**FlowLog** objects. For details, see **Table 4-334**.

Table 4-334 Description of the **FlowLog** field

Parameter	Mandatory	Type	Description
name	No	String	• Flow log name • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	• Flow log description • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
admin_state	No	Boolean	• Whether to enable the flow log function

Example Request

- Change the name of the VPC flow log whose ID is f49f00f1-0f15-470a-a8c5-4e879e461c8d to **flow-log-update**.

```
PUT https://{Endpoint}/v1/b2782e6708b8475c993e6064bc456bf8/fl/flow_logs/f49f00f1-0f15-470a-a8c5-4e879e461c8d
```



```
{
   "flow_log": {
      "name": "flow-log-update",
      "description": "update",
      "admin_state": false
   }
}
```

Response Parameters

Table 4-335 Response parameter

Parameter	Type	Description
flow_log	**flow_log** object	**FlowLog** objects. For details, see **Table 4-336**.

Table 4-336 Description of the **FlowLog** field

Parameter	Type	Description
id	String	• Flow log ID
name	String	• Flow log name • The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
tenant_id	String	• Project ID
description	String	• Flow log description • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
resource_type	String	• Type of the resource for which that the logs to be collected. • The value can be: – **port**: NIC – **vpc**: All NICs in a VPC – **network**: All NICs in a subnet
resource_id	String	• ID of the resource for which that the logs to be collected.

Parameter	Type	Description
traffic_type	String	• Type of the traffic for which that the logs to be collected. • The value can be: – **all**: specifies that both accepted and rejected traffic of the specified resource will be logged. – **accept**: specifies that only accepted inbound and outbound traffic of the specified resource will be logged. – **reject**: specifies that only rejected inbound and outbound traffic of the specified resource will be logged.
log_group_id	String	• Log group ID
log_topic_id	String	• Log topic ID
log_store_type	String	• Service that is used to store flow logs • The value can be: – **lts**: Log Tank Service (LTS)
admin_state	Boolean	• Whether to enable the flow log function
status	String	• Flow log status • The value can be: – **ACTIVE**: Enabled – **DOWN**: Disabled – **ERROR**: Abnormal
created_at	String	• Time when the flow log is created • UTC time in the format of yyyy-MM-ddTHH:mmss
updated_at	String	• Time when the flow log is updated • UTC time in the format of yyyy-MM-ddTHH:mmss

Example Response

```
{
   "flow_log": {
      "id": "f49f00f1-0f15-470a-a8c5-4e879e461c8d",
      "name": " flow-log-update",
      "description": "update",
      "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
      "resource_type": "port",
      "resource_id": "05c4052d-8d14-488f-aa00-19fea5a25fde",
      "traffic_type": "reject",
      "log_group_id": "05c4052d-8d14-488f-aa00-19fea5a25fdd",
      "log_topic_id": "a9d7dee7-37d2-4cba-a208-a016252aaa63",
```



```
    "log_store_type": "lts",
    "created_at": "2019-01-14T11:03:02",
    "updated_at": "2019-01-14T12:03:02",
    "status": "DOWN",
    "admin_state": false
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

4.14.5 Deleting a VPC Flow Log

Function

This API is used to delete a flow log.

URI

DELETE /v1/{project_id}/fl/flow_logs/{flowlog_id}

Table 4-337 describes the parameters.

Table 4-337 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
flowlog_id	Yes	String	Flow log ID

Request Parameters

None

Example Request

```
DELETE https://{Endpoint}/v1/b2782e6708b8475c993e6064bc456bf8/fl/flow_logs/60c809cb-6731-45d0-ace8-3bf5626421a9
```

Response Parameters

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5 API V3

5.1 VPC

5.1.1 Querying VPCs

Function

This API is used to query VPCs.

This API is available in CN North-Beijing1, CN North-Beijing2, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, TR-Istanbul, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago.

Constraints

This API is used to query all VPCs accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query. If the number of records exceeds 2000, the pagination marker will be returned.

URI

GET /v3/{project_id}/vpc/vpcs

Table 5-1 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Table 5-2 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. Value range: 0 to 2000
marker	No	String	Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.
id	No	Array of strings	VPC ID, which can be used to filter VPCs.
name	No	Array of strings	VPC name, which can be used to filter VPCs.
description	No	Array of strings	Supplementary information about the VPC, which can be used to filter VPCs.
cidr	No	Array of strings	VPC CIDR block, which can be used to filter VPCs.

Request Parameter

None

Example Request

- Querying VPCs
  ```
  GET https://{Endpoint}/v3/{project_id}/vpc/vpcs
  ```
- Querying VPCs by VPC ID
  ```
  GET https://{Endpoint}/v3/{project_id}/vpc/vpcs?
  id=01ab4be1-4447-45fb-94be-3ee787ed4ebe&id=02cd5ef2-4447-36fb-75be-3ee787ed6adf
  ```
- Querying VPCs by VPC name
  ```
  GET https://{Endpoint}/v3/{project_id}/vpc/vpcs?name=vpc-test
  ```
- Querying VPCs by page
  ```
  GET https://{Endpoint}/v3/{project_id}/vpc/vpcs?
  limit=2&marker=01ab4be1-4447-45fb-94be-3ee787ed4ebe
  ```

Response Parameter

Table 5-3 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
vpcs	Array of **Vpc** objects	Response body of VPCs

Parameter	Type	Description
page_info	PageInfo object	Pagination information

Table 5-4 Vpc

Parameter	Type	Description
id	String	• VPC ID, which uniquely identifies the VPC. • The value is in UUID format with hyphens (-).
name	String	• VPC name • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about the VPC. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
cidr	String	• Available VPC CIDR blocks • The value can be: – 10.0.0.0/8-10.255.255.240/28 – 172.16.0.0/12-172.31.255.240/28 – 192.168.0.0/16-192.168.255.240/28 – If **cidr** is not specified, the default value is **""**. • The value must be in IPv4 CIDR format, for example, **192.168.0.0/16**.
extend_cidrs	Array of strings	• Secondary CIDR blocks of VPCs • Currently, only IPv4 CIDR blocks are supported.
status	String	• VPC status • The value can be: – **PENDING**: The VPC is being created. – **ACTIVE**: The VPC is created successfully.
project_id	String	ID of the project to which the VPC belongs

Parameter	Type	Description
enterprise_project_id	String	• ID of the enterprise project to which the VPC belongs • The value can be **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
created_at	String	• Time when the VPC is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	• Time when the VPC is updated • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
cloud_resources	Array of **CloudResource** objects	• Type and number of resources associated with the VPC • Currently, only route tables and subnets of the VPC are returned. The number of **virsubnets** is the total number of IPv4 and IPv6 subnets.
tags	Array of **Tag** objects	• VPC tags. For details, see the tag objects. • Value range: 0 to 20 tag key-value pairs

Table 5-5 CloudResource

Parameter	Type	Description
resource_type	String	Resource type
resource_count	Integer	Number of resources

Table 5-6 Tag

Parameter	Type	Description
key	String	Tag key Value range: ● Each key can contain up to 36 Unicode characters and cannot be left blank. ● The value can contain: – Letters – Digits – Special characters: underscores (_) and hyphens (-) – Chinese characters
value	String	Tag value Value range: ● Each value can contain up to 43 Unicode characters and can be left blank. ● The value can contain: – Letters – Digits – Special characters: underscore (_), dot (.), and hyphen (-) – Chinese characters

Table 5-7 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page
current_count	Integer	Total number of records on the current page
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Example Response


```
{
   "request_id": "9c1838ba498249547be43dd618b58d27",
   "vpcs": [
      {
         "id": "01da5a65-0bb9-4638-8ab7-74c64e24a9a7",
         "name": "API-PERF-TEST-14bd44c121",
         "description": "",
         "cidr": "192.168.0.0/16",
```



```
        "extend_cidrs": [ ],
        "status": "ACTIVE",
        "project_id": "087679f0aa80d32a2f4ec0172f5e902b",
        "enterprise_project_id": "0",
        "tags": [ ],
        "created_at": "2020-06-16T02:32:18Z",
        "updated_at": "2020-06-16T02:32:18Z",
        "cloud_resources": [
            {
                "resource_type": "routetable",
                "resource_count": 1
            },
            {
                "resource_type": "virsubnet",
                "resource_count": 0
            }
        ]
    },
    {
        "id": "43fd79b0-f7d7-4e9b-828b-2d4d7bfae428",
        "name": "API-PERF-TEST_m2n33",
        "description": "",
        "cidr": "192.168.0.0/16",
        "extend_cidrs": [ ],
        "status": "ACTIVE",
        "project_id": "087679f0aa80d32a2f4ec0172f5e902b",
        "enterprise_project_id": "0",
        "tags": [ ],
        "created_at": "2020-06-15T06:29:40Z",
        "updated_at": "2020-06-15T06:29:41Z",
        "cloud_resources": [
            {
                "resource_type": "routetable",
                "resource_count": 1
            },
            {
                "resource_type": "virsubnet",
                "resource_count": 1
            }
        ]
    },
    {
        "id": "5ed053ba-b46c-4dce-a1ae-e9d8a7015f21",
        "name": "API-PERF-TEST-c34b1c4b12",
        "description": "",
        "cidr": "192.168.0.0/16",
        "extend_cidrs": [ ],
        "status": "ACTIVE",
        "project_id": "087679f0aa80d32a2f4ec0172f5e902b",
        "enterprise_project_id": "0",
        "tags": [ ],
        "created_at": "2020-06-16T02:32:33Z",
        "updated_at": "2020-06-16T02:32:33Z",
        "cloud_resources": [
            {
                "resource_type": "routetable",
                "resource_count": 1
            },
            {
                "resource_type": "virsubnet",
                "resource_count": 0
            }
        ]
    }
],
"page_info": {
    "previous_marker": "01da5a65-0bb9-4638-8ab7-74c64e24a9a7",
    "current_count": 3
```



```
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.1.2 Querying Details About a VPC

Function

This API is used to query details about a VPC.

URI

GET /v3/{project_id}/vpc/vpcs/{vpc_id}

Table 5-8 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
vpc_id	Yes	String	VPC ID.

Request Parameter

None

Example Request

- Querying details about a VPC

```
"GET https://{Endpoint}/v3/{project_id}/vpc/vpcs/99d9d709-8478-4b46-9f3f-2206b1023fd3"
```

Response Parameter

Table 5-9 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
vpc	**Vpc** object	VPC response body

Table 5-10 Vpc

Parameter	Type	Description
id	String	VPC ID, which uniquely identifies the VPC The value is in UUID format with hyphens (-).
name	String	VPC name The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the VPC. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
cidr	String	Available VPC CIDR blocks Value range: ● 10.0.0.0/8-10.255.255.240/28 ● 172.16.0.0/12-172.31.255.240/28 ● 192.168.0.0/16-192.168.255.240/28 If **cidr** is not specified, the default value is **""**. The value must be in IPv4 CIDR format, for example, **192.168.0.0/16**.
extend_cidrs	Array of strings	Secondary CIDR blocks of VPCs Currently, only IPv4 CIDR blocks are supported.
status	String	VPC status Value range: ● **PENDING**: The VPC is being created. ● **ACTIVE**: The VPC is created successfully.
project_id	String	ID of the project to which the VPC belongs
enterprise_project_id	String	ID of the enterprise project to which the VPC belongs The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
created_at	String	Time when the VPC is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the VPC is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Parameter	Type	Description
cloud_resources	Array of **CloudResource** objects	Type and number of resources associated with the VPC Currently, only route tables and subnets of the VPC are returned. The number of **virsubnets** is the total number of IPv4 and IPv6 subnets.
tags	Array of **Tag** objects	VPC tags. For details, see the tag objects. Value range: 0 to 20 tag key-value pairs

Table 5-11 CloudResource

Parameter	Type	Description
resource_type	String	Resource type
resource_count	Integer	Number of resources

Table 5-12 Tag

Parameter	Type	Description
key	String	Tag key Value range: • Each key can contain up to 36 Unicode characters and cannot be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_) and hyphens (-) – Chinese characters
value	String	Tag value Value range: • Each value can contain up to 43 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscore (_), dot (.), and hyphen (-) – Chinese characters

Example Response


```
{
   "request_id": "84eb4f775d66dd916db121768ec55626",
   "vpc": {
      "id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
      "name": "name-test",
      "description": "description-test",
      "cidr": "192.168.0.0/16",
      "extend_cidrs": [
         "21.8.0.0/16"
      ],
      "enterprise_project_id": "0",
      "tags": [
         {
            "key": "key",
            "value": "value"
         }
      ],
      "cloud_resources": [
         {
            "resource_type": "routetable",
            "resource_count": 1
         }
      ],
      "status": "ACTIVE",
      "project_id": "060576782980d5762f9ec014dd2f1148",
      "created_at": "2018-03-23T09:26:08Z",
      "updated_at": "2018-08-24T08:49:53Z"
   }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.1.3 Adding a Secondary CIDR Block to a VPC

Function

This API is used to add a secondary CIDR block to a VPC.

URI

PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/add-extend-cidr

Table 5-13 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	VPC ID.

Request Parameter

Table 5-14 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Whether to only send the check request. Value range: • **true**: Only the check request will be sent and no secondary CIDR block will be added. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • **false** (default value): A request will be sent and a secondary CIDR block will be added.
vpc	Yes	**AddExtendCidrOption** object	Request body for adding a secondary CIDR block.

Table 5-15 AddExtendCidrOption

Parameter	Mandatory	Type	Description
extend_cidrs	Yes	Array of strings	Secondary CIDR blocks that can be added to VPCs The value cannot contain the following: • 100.64.0.0/10 • 214.0.0.0/7 • 198.18.0.0/15 • 169.254.0.0/16 • 0.0.0.0/8 • 127.0.0.0/8 • 240.0.0.0/4 • 172.31.0.0/16 • 192.168.0.0/16 • 255.255.255.255/32

Example Request

- Add a secondary CIDR block 23.8.0.0/16 to the VPC whose ID is 99d9d709-8478-4b46-9f3f-2206b1023fd3.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/vpcs/99d9d709-8478-4b46-9f3f-2206b1023fd3/add-extend-cidr

{
    "vpc": {
        "extend_cidrs": [
            "23.8.0.0/16"
        ]
    }
}
```

Response Parameter

Table 5-16 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
vpc	Vpc object	Response body of adding a secondary CIDR block

Table 5-17 Vpc

Parameter	Type	Description
id	String	VPC ID that uniquely identifies the VPC The value is in UUID format with hyphens (-).
name	String	VPC name The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the VPC. The value can contain up to 255 characters and cannot contain angle brackets (< or >).
cidr	String	Available VPC CIDR blocks Value range: ● 10.0.0.0/8-10.255.255.240/28 ● 172.16.0.0/12-172.31.255.240/28 ● 192.168.0.0/16-192.168.255.240/28 If **cidr** is not specified, the default value is **""**. The value must be in IPv4 CIDR format, for example, **192.168.0.0/16**.
extend_cidrs	Array of strings	Secondary CIDR blocks of VPCs Currently, only IPv4 CIDR blocks are supported.
status	String	VPC status Value range: ● **PENDING**: The VPC is being created. ● **ACTIVE**: The VPC is created successfully.
project_id	String	ID of the project to which the VPC belongs
enterprise_project_id	String	ID of the enterprise project to which the VPC belongs The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
created_at	String	Time when the VPC is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the VPC is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Parameter	Type	Description
cloud_resources	Array of **CloudResource** objects	Type and number of resources associated with the VPC Currently, only route tables and subnets of the VPC are returned. The number of **virsubnets** is the total number of IPv4 and IPv6 subnets.
tags	Array of **Tag** objects	VPC tags. For details, see the tag objects. Value range: 0 to 20 tag key-value pairs

Table 5-18 CloudResource

Parameter	Type	Description
resource_type	String	Resource type
resource_count	Integer	Number of resources

Table 5-19 Tag

Parameter	Type	Description
key	String	Tag key Value range: • Each key can contain up to 36 Unicode characters and cannot be left blank. • The value can contain: – Letters – Digits – Special characters: underscores (_) and hyphens (-) – Chinese characters
value	String	Tag value Value range: • Each value can contain up to 43 Unicode characters and can be left blank. • The value can contain: – Letters – Digits – Special characters: underscore (_), dot (.), and hyphen (-) – Chinese characters

Example Response


```
{
   "request_id": "84eb4f775d66dd916db121768ec55626",
   "vpc": {
      "id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
      "name": "vpc1",
      "description": "test1",
      "cidr": "192.168.0.0/16",
      "extend_cidrs": [
         "23.8.0.0/16"
      ],
      "enterprise_project_id": "0",
      "tags": [
         {
            "key": "key",
            "value": "value"
         }
      ],
      "cloud_resources": [
         {
            "resource_type": "routetable",
            "resource_count": 1
         }
      ],
      "status": "ACTIVE",
      "project_id": "060576782980d5762f9ec014dd2f1148",
      "created_at": "2018-03-23T09:26:08Z",
      "updated_at": "2018-08-24T08:49:53Z"
   }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.1.4 Removing a Secondary CIDR Block from a VPC

Function

This API is used to remove a secondary CIDR block from a VPC.

URI

PUT /v3/{project_id}/vpc/vpcs/{vpc_id}/remove-extend-cidr

Table 5-20 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	VPC ID.

Request Parameter

Table 5-21 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Whether to only send the check request. Value range: • **true**: Only the check request will be sent and no secondary CIDR block will be added. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • **false** (default value): A request will be sent and a secondary CIDR block will be added.
vpc	Yes	**RemoveExtendCidrOption** object	Request body for removing a secondary CIDR block

Table 5-22 RemoveExtendCidrOption

Parameter	Mandatory	Type	Description
extend_cidrs	Yes	Array of strings	Secondary CIDR blocks that can be removed from VPCs VPCs already have secondary CIDR blocks. Constraints: • Before removing a secondary CIDR block, delete the subnets in the CIDR block first.

Example Request

- Remove the secondary CIDR block 23.8.0.0/16 from the VPC whose ID is 99d9d709-8478-4b46-9f3f-2206b1023fd3.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/vpcs/99d9d709-8478-4b46-9f3f-2206b1023fd3/remove-extend-cidr

{
    "vpc": {
        "extend_cidrs": [
            "23.8.0.0/16"
        ]
    }
}
```

Response Parameter

Table 5-23 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
vpc	**Vpc** object	Response body of removing a secondary CIDR block

Table 5-24 Vpc

Parameter	Type	Description
id	String	VPC ID that uniquely identifies the VPC The value is in UUID format with hyphens (-).
name	String	VPC name The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the VPC. The value can contain up to 255 characters and cannot contain angle brackets (< or >).
cidr	String	Available VPC CIDR blocks Value range: • 10.0.0.0/8-10.255.255.240/28 • 172.16.0.0/12-172.31.255.240/28 • 192.168.0.0/16-192.168.255.240/28 If **cidr** is not specified, the default value is **""**. • The value must be in IPv4 CIDR format, for example, **192.168.0.0/16**.

Parameter	Type	Description
extend_cidrs	Array of strings	Secondary CIDR blocks of VPCs Currently, only IPv4 CIDR blocks are supported.
status	String	VPC status Value range: • **PENDING**: The VPC is being created. • **ACTIVE**: The VPC is created successfully.
project_id	String	ID of the project to which the VPC belongs
enterprise_project_id	String	ID of the enterprise project to which the VPC belongs The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
created_at	String	Time when the VPC is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the VPC is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
cloud_resources	Array of **CloudResource** objects	Type and number of resources associated with the VPC Currently, only route tables and subnets of the VPC are returned. The number of **virsubnets** is the total number of IPv4 and IPv6 subnets.
tags	Array of **Tag** objects	VPC tags. For details, see the tag objects. Value range: 0 to 20 tag key-value pairs

Table 5-25 CloudResource

Parameter	Type	Description
resource_type	String	Resource type
resource_count	Integer	Number of resources

Table 5-26 Tag

Parameter	Type	Description
key	String	Tag key Value range: ● Each key can contain up to 36 Unicode characters and cannot be left blank. ● The value can contain: – Letters – Digits – Special characters: underscores (_) and hyphens (-) – Chinese characters
value	String	Tag value Value range: ● Each value can contain up to 43 Unicode characters and can be left blank. ● The value can contain: – Letters – Digits – Special characters: underscore (_), dot (.), and hyphen (-) – Chinese characters

Example Response

```
{
   "request_id": "84eb4f775d66dd916db121768ec55626",
   "vpc": {
      "id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
      "name": "vpc1",
      "description": "test1",
      "cidr": "192.168.0.0/16",
      "extend_cidrs": [ ],
      "enterprise_project_id": "0",
      "tags": [
         {
            "key": "key",
            "value": "value"
         }
      ],
      "cloud_resources": [
         {
            "resource_type": "routetable",
            "resource_count": 1
         }
      ],
      "status": "ACTIVE",
      "project_id": "060576782980d5762f9ec014dd2f1148",
      "created_at": "2018-03-23T09:26:08Z",
      "updated_at": "2018-08-24T08:49:53Z"
   }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.2 Security Group

5.2.1 Creating a Security Group

Function

This API is used to create a security group.

Constraints

By default, a security group only allows instances in it to communicate with each other.

URI

POST /v3/{project_id}/vpc/security-groups

Table 5-27 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameter

Table 5-28 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Whether to only send the check request. The value can be: • **true**: A check request will be sent and no security group will be created. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • **false** (default value): A request will be sent and a security group will be created.
security_group	Yes	**CreateSecurityGroupOption** object	Request body for creating a security group

Table 5-29 CreateSecurityGroupOption

Parameter	Mandatory	Type	Description
name	Yes	String	Security group name The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. When creating a security group, associate the enterprise project ID with the security group. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	No	Array of **ResourceTag** objects	Security group tags

Table 5-30 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value Maximum length: **255**

Example Request

- Create a security group and set its name to **security_group_1** and description to **security group description**.

```
"POST https://{Endpoint}/v3/{project_id}/vpc/security-groups"

{
    "security_group": {
        "name": "security_group_1",
        "description": "security group description"
    }
}
```

- Create a security group, set its name to **security_group_1** and description to **security group description**, and specify that the request is pre-checked.

```
"POST https://{Endpoint}/v3/{project_id}/vpc/security-groups"

{
    "security_group": {
        "name": "security_group_1",
        "description": "security group description",
        "tags": [{
          "key": "key1",
```



```
        "value": "value1"
      }]
  },
  "dry_run": true
}
```

Response Parameter

When the status code is **201**, the response parameters are as follows:

Table 5-31 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
security_group	**SecurityGroupInfo** object	Response body for creating a security group

Table 5-32 SecurityGroupInfo

Parameter	Type	Description
id	String	Security group ID, which uniquely identifies the security group The value is in UUID format with hyphens (-).
name	String	Security group name The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project to which the security group belongs
created_at	String	Time when the security group is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Parameter	Type	Description
enterprise_project_id	String	ID of the enterprise project to which the security group belongs The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Security group tags
security_group_rules	Array of **SecurityGroupRule** object	Security group rules

Table 5-33 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value Maximum length: **255**

Table 5-34 SecurityGroupRule

Parameter	Type	Description
id	String	Security group rule ID, which uniquely identifies the security group rule The value is in UUID format with hyphens (-).
description	String	Provides supplementary information about the security group rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	ID of the security group to which the security group rule belongs.

Parameter	Type	Description
direction	String	Inbound or outbound direction of a security group rule. The value can be: • **ingress**: inbound direction • **egress**: outbound direction
protocol	String	Protocol type The value can be **icmp**, **tcp**, **udp**, **icmpv6** or an IP number. If the parameter is left blank, all protocols are supported. When the protocol is **icmpv6**, IP version should be **IPv6**. When the protocol is **icmp**, IP version should be **IPv4**.
ethertype	String	IP version The value can be **IPv4** or **IPv6**. If you do not set this parameter, **IPv4** is used by default.
multiport	String	Port or port range The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).
action	String	Action of the security group rule. The value can be: • **allow** • **deny** The default value is **deny**.
priority	Integer	Rule priority. The value is from **1** to **100**. The value **1** indicates the highest priority.
remote_group_id	String	ID of the remote security group, which allows or denies traffic to and from the security group. Value range: ID of an existing security group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_address_group_id**.

Parameter	Type	Description
remote_ip_prefix	String	Remote IP address. • If **direction** is set to **egress**, the parameter specifies the source IP address. • If **direction** is set to **ingress**, the parameter specifies the destination IP address. The value is an IP address or a CIDR block. The parameter is mutually exclusive with parameters **remote_group_id** and **remote_address_group_id**.
remote_address_group_id	String	ID of the remote IP address group. Value range: ID of an existing IP address group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
created_at	String	Time when the security group rule is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group rule is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	ID of the project to which the security group rule belongs.

When the status code is **400**, the response parameters are as follows:

Table 5-35 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **401**, the response parameters are as follows:

Table 5-36 Response body parameters

Parameter	Type	Description
request_id	String	Request ID

Parameter	Type	Description
error_msg	String	Error message
error_code	String	Error code

When the status code is **403**, the response parameters are as follows:

Table 5-37 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **409**, the response parameters are as follows:

Table 5-38 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **500**, the response parameters are as follows:

Table 5-39 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Response

When the status code is **201**, the response parameters are as follows:

Created

```
{
    "security_group": {
```



```
"id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
"name": "security_group_1",
"project_id": "060576782980d5762f9ec014dd2f1148",
"description": "security group description",
"enterprise_project_id": "0",
"security_group_rules": [
    {
        "id": "f11a3824-ac19-4fad-b4f1-c5f4a6dd0a80",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
        "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
        "direction": "ingress",
        "protocol": null,
        "description": "",
        "created_at": "2020-07-09T05:56:27Z",
        "updated_at": "2020-07-09T05:56:27Z",
        "ethertype": "IPv6",
        "remote_ip_prefix": null,
        "multiport": null,
        "remote_address_group_id": null,
        "action": "allow",
        "priority": 100
    },
    {
        "id": "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
        "remote_group_id": null,
        "direction": "egress",
        "protocol": null,
        "description": "",
        "created_at": "2020-07-09T05:56:27Z",
        "updated_at": "2020-07-09T05:56:27Z",
        "ethertype": "IPv6",
        "remote_ip_prefix": null,
        "multiport": null,
        "remote_address_group_id": null,
        "action": "allow",
        "priority": 100
    },
    {
        "id": "9581f18c-1fdd-43da-ace9-7758a56ef28a",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
        "remote_group_id": null,
        "direction": "egress",
        "protocol": null,
        "description": "",
        "created_at": "2020-07-09T05:56:27Z",
        "updated_at": "2020-07-09T05:56:27Z",
        "ethertype": "IPv4",
        "remote_ip_prefix": null,
        "multiport": null,
        "remote_address_group_id": null,
        "action": "allow",
        "priority": 100
    },
    {
        "id": "a3ba270e-e58b-432d-a912-aeb7eace9fb8",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
        "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
        "direction": "ingress",
        "protocol": null,
        "description": "",
        "created_at": "2020-07-09T05:56:27Z",
        "updated_at": "2020-07-09T05:56:27Z",
        "ethertype": "IPv4",
        "remote_ip_prefix": null,
```



```
            "multiport": null,
            "remote_address_group_id": null,
            "action": "allow",
            "priority": 100
        }
    ],
    "created_at": "2020-07-09T05:56:27Z",
    "updated_at": "2020-07-09T05:56:27Z"
  },
  "request_id": "a8cf4f79ca3c22ca685e7e8872e8c20b"
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.2.2 Querying Security Groups

Function

This API is used to query all security groups of a tenant.

Constraints

This API is used to query all security groups accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query. If the number of records exceeds 2000, the pagination marker will be returned.

URI

GET /v3/{project_id}/vpc/security-groups

Table 5-40 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Table 5-41 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. Value range: 0 to 2000
marker	No	String	Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.
id	No	String	Security group ID. This field can be used to precisely filter security groups. Multiple IDs can be specified for filtering.
name	No	Array of strings	Security group name. This field can be used to precisely filter security groups. Multiple names can be specified for filtering.
description	No	Array of strings	Supplementary information about the security group. This field can be used to precisely filter security groups. Multiple descriptions can be specified for filtering.
enterprise_project_id	No	String	Enterprise project ID. This field can be used to filter the security groups of an enterprise project. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. To obtain the security groups bound to all enterprise projects of the user, set **all_granted_eps**.

Request Parameter

None

Example Request

- Query security groups.
  GET https://{Endpoint}/v3/{project_id}/vpc/security-groups

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-42 Response body parameters

Parameter	Type	Description
security_groups	Array of **SecurityGroup** objects	Response body of security groups
request_id	String	Request ID
page_info	**PageInfo** object	Pagination information

Table 5-43 SecurityGroup

Parameter	Type	Description
id	String	Security group ID, which uniquely identifies the security group The value is in UUID format with hyphens (-).
name	String	Security group name The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Supplementary information about the security group The value can contain up to 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project to which the security group belongs
created_at	String	Time when the security group is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
enterprise_project_id	String	ID of the enterprise project to which the security group belongs The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Security group tags

Table 5-44 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value Maximum length: **255**

Table 5-45 page_info

Parameter	Type	Description
previous_marker	String	First record on the current page
current_count	Integer	Total number of records on the current page
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

When the status code is **400**, the response parameters are as follows:

Table 5-46 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **401**, the response parameters are as follows:

Table 5-47 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **403**, the response parameters are as follows:

Table 5-48 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **500**, the response parameters are as follows:

Table 5-49 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Response

When the status code is **200**, the response parameters are as follows:

OK

```
{
   "request_id": "d31cb32ca06f3c1a294fa24e6cbc5a56",
   "security_groups": [
      {
         "id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
         "name": "Sys-FullAccess--",
         "project_id": "060576782980d5762f9ec014dd2f1148",
         "description": "~!@#¥",
         "enterprise_project_id": "0",
         "created_at": "2019-10-16T11:11:14Z",
         "updated_at": "2020-03-25T10:53:46Z",
         "tags": []

      },
      {
         "id": "0b8cb773-197c-4c91-94f1-e051f0563e5a",
         "name": "test-sg",
         "project_id": "060576782980d5762f9ec014dd2f1148",
         ""description": "The security group is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 3389, 80, and 443. This security group is suitable for ECSs that require remote login, public network ping, and website services.",
         "enterprise_project_id": "0",
         "created_at": "2019-12-03T09:02:11Z",
         "updated_at": "2019-12-03T09:02:11Z",
         "tags": []
      }
```



```
  ],
  "page_info": {
     "previous_marker": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
     "current_count": 2
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.2.3 Querying a Security Group

Function

This API is used to query details about a security group.

URI

GET /v3/{project_id}/vpc/security-groups/{security_group_id}

Table 5-50 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
security_group_id	Yes	String	Security group ID.

Request Parameter

None

Example Request

- Query details about a security group.
  "GET https://{Endpoint}/v3/{project_id}/vpc/security-groups/1d8b19c7-7c56-48f7-a99b-4b40eb390967"

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-51 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
security_group	**SecurityGroupInfo** object	Response body for querying details about a security group

Table 5-52 SecurityGroupInfo

Parameter	Type	Description
id	String	Security group ID, which uniquely identifies the security group The value is in UUID format with hyphens (-).
name	String	Security group name The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project to which the security group belongs
created_at	String	Time when the security group is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
enterprise_project_id	String	ID of the enterprise project to which the security group belongs The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Security group tags

Parameter	Type	Description
security_group_rules	Array of **SecurityGroupRule** objects	Security group rules

Table 5-53 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value Maximum length: **255**

Table 5-54 SecurityGroupRule

Parameter	Type	Description
id	String	Security group rule ID, which uniquely identifies the security group rule The value is in UUID format with hyphens (-).
description	String	Provides supplementary information about the security group rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	ID of the security group to which the security group rule belongs.
direction	String	Inbound or outbound direction of a security group rule. The value can be: • **ingress**: inbound direction • **egress**: outbound direction

Parameter	Type	Description
protocol	String	Protocol type The value can be **icmp**, **tcp**, **udp**, **icmpv6** or an IP number. If the parameter is left blank, all protocols are supported. When the protocol is **icmpv6**, IP version should be **IPv6**. When the protocol is **icmp**, IP version should be **IPv4**.
ethertype	String	IP version The value can be **IPv4** or **IPv6**. If you do not set this parameter, **IPv4** is used by default.
multiport	String	Port or port range The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).
action	String	Action of the security group rule. The value can be: • **allow** • **deny** The default value is **deny**.
priority	Integer	Rule priority. The value is from **1** to **100**. The value **1** indicates the highest priority.
remote_group_id	String	ID of the remote security group, which allows or denies traffic to and from the security group. Value range: ID of an existing security group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_address_group_id**.
remote_ip_prefix	String	Remote IP address. • If **direction** is set to **egress**, the parameter specifies the source IP address. • If **direction** is set to **ingress**, the parameter specifies the destination IP address. The value is an IP address or a CIDR block. The parameter is mutually exclusive with parameters **remote_group_id** and **remote_address_group_id**.

Parameter	Type	Description
remote_address_group_id	String	ID of the remote IP address group. Value range: ID of an existing IP address group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
created_at	String	Time when the security group rule is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group rule is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	ID of the project to which the security group rule belongs.

When the status code is **401**, the response parameters are as follows:

Table 5-55 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **403**, the response parameters are as follows:

Table 5-56 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **404**, the response parameters are as follows:

Table 5-57 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **500**, the response parameters are as follows:

Table 5-58 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Response

When the status code is **200**, the response parameters are as follows:

OK


```
{
   "security_group": {
      "id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
      "name": "security_group_1",
      "project_id": "060576782980d5762f9ec014dd2f1148",
      "description": "security group description",
      "enterprise_project_id": "0",
      "security_group_rules": [
         {
            "id": "f11a3824-ac19-4fad-b4f1-c5f4a6dd0a80",
            "project_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "direction": "ingress",
            "protocol": null,
            "description": "",
            "created_at": "2020-07-09T05:56:27Z",
            "updated_at": "2020-07-09T05:56:27Z",
            "ethertype": "IPv6",
            "remote_ip_prefix": null,
            "multiport": null,
            "remote_address_group_id": null,
            "action": "allow",
            "priority": 100
         },
         {
            "id": "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
            "project_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": null,
            "direction": "egress",
            "protocol": null,
            "description": "",
```



```
            "created_at": "2020-07-09T05:56:27Z",
            "updated_at": "2020-07-09T05:56:27Z",
            "ethertype": "IPv6",
            "remote_ip_prefix": null,
            "multiport": null,
            "remote_address_group_id": null,
            "action": "allow",
            "priority": 100
        },
        {
            "id": "9581f18c-1fdd-43da-ace9-7758a56ef28a",
            "project_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": null,
            "direction": "egress",
            "protocol": null,
            "description": "",
            "created_at": "2020-07-09T05:56:27Z",
            "updated_at": "2020-07-09T05:56:27Z",
            "ethertype": "IPv4",
            "remote_ip_prefix": null,
            "multiport": null,
            "remote_address_group_id": null,
            "action": "allow",
            "priority": 100
        },
        {
            "id": "a3ba270e-e58b-432d-a912-aeb7eace9fb8",
            "project_id": "060576782980d5762f9ec014dd2f1148",
            "security_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "remote_group_id": "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
            "direction": "ingress",
            "protocol": null,
            "description": "",
            "created_at": "2020-07-09T05:56:27Z",
            "updated_at": "2020-07-09T05:56:27Z",
            "ethertype": "IPv4",
            "remote_ip_prefix": null,
            "multiport": null,
            "remote_address_group_id": null,
            "action": "allow",
            "priority": 100
        }
    ],
    "created_at": "2020-07-09T05:56:27Z",
    "updated_at": "2020-07-09T05:56:27Z",
    "tags": []
  },
  "request_id": "a8cf4f79ca3c22ca685e7e8872e8c20b"
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.2.4 Updating a Security Group

Function

This API is used to update a security group.

URI

PUT /v3/{project_id}/vpc/security-groups/{security_group_id}

Table 5-59 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
security_group_id	Yes	String	Security group ID.

Request Parameter

Table 5-60 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Whether to only send the check request. The value can be: • **true**: A check request will be sent and no security group will be updated. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • **false** (default value): A request will be sent and a security group will be updated.
security_group	Yes	**UpdateSecurityGroupOption** object	Request body for updating a security group

Table 5-61 UpdateSecurityGroupOption

Parameter	Mandatory	Type	Description
name	No	String	Security group name The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Example Request

- Change the name of the security group whose ID is 1d8b19c7-7c56-48f7-a99b-4b40eb390967 to **security_group_2** and its description to **modified description**.

```
"PUT https://{Endpoint}/v3/{project_id}/vpc/security-groups/1d8b19c7-7c56-48f7-a99b-4b40eb390967"

{
  "security_group" : {
    "name" : "security_group_2",
    "description" : "modified description"
  }
}
```

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-62 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
security_group	**SecurityGroupInfo** object	Response body for updating a security group

Table 5-63 SecurityGroupInfo

Parameter	Type	Description
id	String	Security group ID, which uniquely identifies the security group The value is in UUID format with hyphens (-).
name	String	Security group name The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project to which the security group belongs
created_at	String	Time when the security group is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
enterprise_project_id	String	ID of the enterprise project to which the security group belongs The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Security group tags
security_group_rules	Array of **SecurityGroupRule** objects	Security group rules

Table 5-64 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value Maximum length: **255**

Table 5-65 SecurityGroupRule

Parameter	Type	Description
id	String	Security group rule ID, which uniquely identifies the security group rule The value is in UUID format with hyphens (-).
description	String	Provides supplementary information about the security group rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	ID of the security group to which the security group rule belongs.
direction	String	Inbound or outbound direction of a security group rule. The value can be: • **ingress**: inbound direction • **egress**: outbound direction
protocol	String	Protocol type The value can be **icmp**, **tcp**, **udp**, **icmpv6** or an IP number. If the parameter is left blank, all protocols are supported. When the protocol is **icmpv6**, IP version should be **IPv6**. When the protocol is **icmp**, IP version should be **IPv4**.
ethertype	String	IP version The value can be **IPv4** or **IPv6**. If you do not set this parameter, **IPv4** is used by default.

Parameter	Type	Description
multiport	String	Port or port range The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).
action	String	Action of the security group rule. The value can be: • **allow** • **deny** The default value is **deny**.
priority	Integer	Rule priority. The value is from **1** to **100**. The value **1** indicates the highest priority.
remote_group_id	String	ID of the remote security group, which allows or denies traffic to and from the security group. Value range: ID of an existing security group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_address_group_id**.
remote_ip_prefix	String	Remote IP address. • If **direction** is set to **egress**, the parameter specifies the source IP address. • If **direction** is set to **ingress**, the parameter specifies the destination IP address. The value is an IP address or a CIDR block. The parameter is mutually exclusive with parameters **remote_group_id** and **remote_address_group_id**.
remote_address_group_id	String	ID of the remote IP address group. Value range: ID of an existing IP address group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
created_at	String	Time when the security group rule is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group rule is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Parameter	Type	Description
project_id	String	ID of the project to which the security group rule belongs.

Example Response

When the status code is **200**, the response parameters are as follows:

OK


```
{
  "security_group" : {
    "id" : "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
    "name" : "security_group_2",
    "project_id" : "060576782980d5762f9ec014dd2f1148",
    "description" : "modified description",
    "enterprise_project_id" : "0",
    "security_group_rules" : [ {
      "id" : "f11a3824-ac19-4fad-b4f1-c5f4a6dd0a80",
      "project_id" : "060576782980d5762f9ec014dd2f1148",
      "security_group_id" : "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
      "remote_group_id" : "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
      "direction" : "ingress",
      "protocol" : null,
      "description" : "",
      "created_at" : "2020-07-09T05:56:27Z",
      "updated_at" : "2020-07-09T05:56:27Z",
      "ethertype" : "IPv6",
      "remote_ip_prefix" : null,
      "multiport" : null,
      "remote_address_group_id" : null,
      "action" : "allow",
      "priority" : 100
    }, {
      "id" : "3d6480e8-9ea4-46dc-bb1b-8db190cd5677",
      "project_id" : "060576782980d5762f9ec014dd2f1148",
      "security_group_id" : "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
      "remote_group_id" : null,
      "direction" : "egress",
      "protocol" : null,
      "description" : "",
      "created_at" : "2020-07-09T05:56:27Z",
      "updated_at" : "2020-07-09T05:56:27Z",
      "ethertype" : "IPv6",
      "remote_ip_prefix" : null,
      "multiport" : null,
      "remote_address_group_id" : null,
      "action" : "allow",
      "priority" : 100
    }, {
      "id" : "9581f18c-1fdd-43da-ace9-7758a56ef28a",
      "project_id" : "060576782980d5762f9ec014dd2f1148",
      "security_group_id" : "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
      "remote_group_id" : null,
      "direction" : "egress",
      "protocol" : null,
      "description" : "",
      "created_at" : "2020-07-09T05:56:27Z",
      "updated_at" : "2020-07-09T05:56:27Z",
      "ethertype" : "IPv4",
      "remote_ip_prefix" : null,
      "multiport" : null,
      "remote_address_group_id" : null,
      "action" : "allow",
```



```
    "priority" : 100
  }, {
    "id" : "a3ba270e-e58b-432d-a912-aeb7eace9fb8",
    "project_id" : "060576782980d5762f9ec014dd2f1148",
    "security_group_id" : "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
    "remote_group_id" : "69c999ad-d9ef-4d79-94fd-35e6ceb75325",
    "direction" : "ingress",
    "protocol" : null,
    "description" : "",
    "created_at" : "2020-07-09T05:56:27Z",
    "updated_at" : "2020-07-09T05:56:27Z",
    "ethertype" : "IPv4",
    "remote_ip_prefix" : null,
    "multiport" : null,
    "remote_address_group_id" : null,
    "action" : "allow",
    "priority" : 100
  } ],
  "created_at" : "2020-07-09T05:56:27Z",
  "updated_at" : "2020-07-09T05:56:27Z",
  "tags": []
 },
 "request_id" : "a8cf4f79ca3c22ca685e7e8872e8c20b"
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.2.5 Deleting a Security Group

Function

This API is used to delete a security group.

Constraints

Before deleting a security group, ensure that the security group is not associated with any instance.

URI

DELETE /v3/{project_id}/vpc/security-groups/{security_group_id}

Table 5-66 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Parameter	Mandatory	Type	Description
security_group_id	Yes	String	Security group ID.

Request Parameter

None

Example Request

- Delete a single security group.
  "DELETE https://{Endpoint}/v3/{project_id}/vpc/security-groups/1d8b19c7-7c56-48f7-a99b-4b40eb390967"

Response Parameter

When the status code is **400**, the response parameters are as follows:

Table 5-67 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **401**, the response parameters are as follows:

Table 5-68 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **403**, the response parameters are as follows:

Table 5-69 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **404**, the response parameters are as follows:

Table 5-70 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **409**, the response parameters are as follows:

Table 5-71 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

When the status code is **500**, the response parameters are as follows:

Table 5-72 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.3 Security Group Rule

5.3.1 Creating a Security Group Rule

Function

This API is used to create a security group rule.

URI

POST /v3/{project_id}/vpc/security-group-rules

Table 5-73 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameter

Table 5-74 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Whether to only send the check request. The value can be: • **true**: A check request will be sent and no security group rule will be created. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. • **false** (default value): A request will be sent and a security group rule will be created.
security_group_rule	Yes	**CreateSecurityGroupRuleOption** object	Request body for creating a security group rule.

Table 5-75 CreateSecurityGroupRuleOption

Parameter	Mandatory	Type	Description
security_group_id	Yes	String	ID of the security group to which the security group rule belongs.
description	No	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
direction	Yes	String	Inbound or outbound direction of a security group rule. The value can be: • **ingress**: inbound direction • **egress**: outbound direction

Parameter	Mandatory	Type	Description
ethertype	No	String	IP version The value can be **IPv4** or **IPv6**. If you do not set this parameter, **IPv4** is used by default.
protocol	No	String	Protocol type The value can be **icmp**, **tcp**, **udp**, **icmpv6** or an IP number (0 to 255). Constraints: • If the parameter is left blank, all protocols are supported. • When the protocol is **icmpv6**, IP version should be **IPv6**. • When the protocol is **icmp**, IP version should be **IPv4**.
multiport	No	String	Port or port range The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80). The port is from 1 to 65535.
remote_ip_prefix	No	String	Remote IP address. If **direction** is set to **egress**, the parameter specifies the source IP address. If **direction** is set to **ingress**, the parameter specifies the destination IP address. The value is an IP address or a CIDR block. Constraints: • The parameter is mutually exclusive with parameters **remote_group_id** and **remote_address_group_id**. • If this parameter is left blank, the remote IP address is not limited, and the traffic from all remote IP addresses is allowed or rejected.

Parameter	Mandatory	Type	Description
remote_group_id	No	String	ID of the remote security group, which allows or denies traffic to and from the security group. Value range: ID of an existing security group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_address_group_id**.
remote_address_group_id	No	String	ID of the remote IP address group. Value range: ID of an existing IP address group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
action	No	String	Action of the security group rule. The value can be: • **allow** • **deny** The default value is **allow**.
priority	No	String	Rule priority in a security group. The value is from **1** to **100**. The value **1** indicates the highest priority. The default value is **1**.

Example Request

- Create an inbound rule in the security group whose ID is 1c8d9f94-6022-4518-bb98-e0145fcc7b33.

```
POST https://{Endpoint}/v3/{project_id}/vpc/security-group-rules

{
   "security_group_rule": {
      "security_group_id": "1c8d9f94-6022-4518-bb98-e0145fcc7b33",
      "direction": "ingress",
      "protocol": "tcp",
      "description": "security group rule description",
      "action": "allow",
      "priority": 1,
      "multiport": "33",
      "remote_ip_prefix": "10.10.0.0/16"
   }
}
```

Response Parameter

When the status code is **201**, the response parameters are as follows:

Table 5-76 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
security_group_rule	**SecurityGroupRule** object	Response body for creating a security group rule.

Table 5-77 SecurityGroupRule

Parameter	Type	Description
id	String	Security group rule ID, which uniquely identifies the security group rule The value is in UUID format with hyphens (-).
description	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	ID of the security group to which the security group rule belongs.
direction	String	Inbound or outbound direction of a security group rule. The value can be: • **ingress**: inbound direction • **egress**: outbound direction
protocol	String	Protocol type The value can be **icmp**, **tcp**, **udp**, **icmpv6** or an IP number. Constraints: • If the parameter is left blank, all protocols are supported. • When the protocol is **icmpv6**, IP version should be **IPv6**. • When the protocol is **icmp**, IP version should be **IPv4**.
ethertype	String	IP version The value can be **IPv4** or **IPv6**. If you do not set this parameter, **IPv4** is used by default.

Parameter	Type	Description
multiport	String	Port or port range The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).
action	String	Action of the security group rule. The value can be: • **allow** • **deny** The default value is **deny**.
priority	Integer	Rule priority. The value is from **1** to **100**. The value **1** indicates the highest priority.
remote_group_id	String	ID of the remote security group, which allows or denies traffic to and from the security group. Value range: ID of an existing security group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_address_group_id**.
remote_ip_prefix	String	Remote IP address. If **direction** is set to **egress**, the parameter specifies the source IP address. If **direction** is set to **ingress**, the parameter specifies the destination IP address. The value is an IP address or a CIDR block. Constraints: • The parameter is mutually exclusive with parameters **remote_group_id** and **remote_address_group_id**. • If this parameter is left blank, the remote IP address is not limited, and the traffic from all remote IP addresses is allowed or rejected.
remote_address_group_id	String	ID of the remote IP address group. Value range: ID of an existing IP address group The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
created_at	String	Time when the security group rule is created UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Parameter	Type	Description
updated_at	String	Time when the security group rule is updated UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	ID of the project to which the security group rule belongs.

Example Response

When the status code is **201**, the response parameters are as follows:

```
{
    "request_id": "1666b2708aaf849337572d6846dce781",
    "security_group_rule": {
        "id": "f626eb24-d8bd-4d26-ae0b-c16bb65730cb",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "security_group_id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
        "remote_group_id": null,
        "direction": "ingress",
        "protocol": "tcp",
        "description": "security group rule description",
        "created_at": "2020-08-13T07:12:36Z",
        "updated_at": "2020-08-13T07:12:36Z",
        "ethertype": "IPv4",
        "remote_ip_prefix": "10.10.0.0/16",
        "multiport": "33",
        "remote_address_group_id": null,
        "action": "allow",
        "priority": 1
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.3.2 Querying Security Group Rules

Function

This API is used to query security group rules.

URI

GET /v3/{project_id}/vpc/security-group-rules

Table 5-78 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Table 5-79 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	• Specifies the number of records returned on each page. • Value range: 0 to 2000
marker	No	String	Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.
id	No	Array of strings	ID of the security group rule. Multiple IDs can be specified for filtering.
security_group_id	No	Array of strings	ID of the security group to which the security group rule belongs. Multiple IDs can be specified for filtering.
protocol	No	Array of strings	Protocol specified in the security group rule. Multiple protocols can be specified for filtering.
description	No	Array of strings	Supplementary information about the security group. This field can be used to precisely filter security groups. Multiple descriptions can be specified for filtering.
remote_group_id	No	Array of strings	ID of the remote security group. Multiple IDs can be specified for filtering.
direction	No	String	• Access control direction specified in the security group rule. • The value can be **ingress** (inbound direction) or **egress** (outbound direction).
action	No	String	Action of the security group rule.

Parameter	Mandatory	Type	Description
remote_ip_prefix	No	String	• Remote IP address. • The value must be in CIDR format.

Request Parameter

None

Example Request

- Query security group rules.
  GET https://{Endpoint}/v3/{project_id}/vpc/security-group-rules

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-80 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
security_group_rules	Array of **SecurityGroupRule** objects	Response body of security group rules
page_info	**PageInfo** object	Pagination information

Table 5-81 SecurityGroupRule

Parameter	Type	Description
id	String	• Security group rule ID, which uniquely identifies the security group rule. • The value is in UUID format with hyphens (-).
description	String	• Supplementary information about the security group. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	• ID of the security group to which the security group rule belongs

Parameter	Type	Description
direction	String	• Inbound or outbound direction of a security group rule. • The value can be **ingress** (inbound direction) or **egress** (outbound direction).
protocol	String	• Protocol type. • The value can be **icmp**, **tcp**, **udp**, **icmpv6** or an IP number. • Constraints: – If the parameter is left blank, all protocols are supported. – When the protocol is **icmpv6**, IP version should be **IPv6**. – When the protocol is **icmp**, IP version should be **IPv4**.
ethertype	String	• IP version. • The value can be **IPv4** or **IPv6**. • If you do not set this parameter, **IPv4** is used by default.
multiport	String	• Port or port range. • The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).
action	String	• Action of the security group rule. • The value can be: – **allow** – **deny** • The default value is **deny**.
priority	Integer	• Rule priority. • The value is from **1** to **100**. The value **1** indicates the highest priority.
remote_group_id	String	• ID of the remote security group, which allows or denies traffic to and from the security group. • Value range: ID of an existing security group • The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_address_group_id**.

Parameter	Type	Description
remote_ip_prefix	String	• Remote IP address. When the direction is **egress**, it is the address of the terminal that accesses the VM. When the direction is **ingress**, it is the address of the VM to be accessed. • The value is an IP address or a CIDR block. • Constraints: – The parameter is mutually exclusive with parameters **remote_group_id** and **remote_address_group_id**. – If this parameter is left blank, the remote IP address is not limited, and the traffic from all remote IP addresses is allowed or rejected.
remote_address_group_id	String	• ID of the remote IP address group. • Value range: ID of an existing IP address group • The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
created_at	String	• Time when the security group rule is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	• Time when the security group rule is updated • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	• ID of the project to which the security group rule belongs.

Table 5-82 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page
current_count	Integer	Total number of records on the current page
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Example Response

When the status code is **200**, the response parameters are as follows:

OK

```
{
   "request_id": "80747d36e3376c0894ba8f9a9156355d",
   "security_group_rules": [
      {
         "id": "f626eb24-d8bd-4d26-ae0b-c16bb65730cb",
         "project_id": "060576782980d5762f9ec014dd2f1148",
         "security_group_id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
         "remote_group_id": null,
         "direction": "ingress",
         "protocol": "tcp",
         "description": "security group rule description",
         "created_at": "2020-08-13T07:12:36Z",
         "updated_at": "2020-08-13T07:12:36Z",
         "ethertype": "IPv4",
         "remote_ip_prefix": "10.10.0.0/16",
         "multiport": "333",
         "remote_address_group_id": null,
         "action": "allow",
         "priority": 1
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.3.3 Querying a Security Group Rule

Function

This API is used to query details about a security group rule.

URI

GET /v3/{project_id}/vpc/security-group-rules/{security_group_rule_id}

Table 5-83 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
security_group_rule_id	Yes	String	Security group rule ID.

Request Parameter

None

Example Request

- Query details about a security group rule.
  ```
  "GET https://{Endpoint}/v3/{project_id}/vpc/security-group-rules/01a772b2-463e-47e3-a95d-bac85ee8adc6"
  ```

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-84 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
security_group_rule	**SecurityGroupRule** object	Response body for querying details about a security group rule

Table 5-85 SecurityGroupRule

Parameter	Type	Description
id	String	• Security group rule ID, which uniquely identifies the security group rule. • The value is in UUID format with hyphens (-).
description	String	• Supplementary information about the security group. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	• ID of the security group to which the security group rule belongs
direction	String	• Inbound or outbound direction of a security group rule. • The value can be **ingress** (inbound direction) or **egress** (outbound direction).

Parameter	Type	Description
protocol	String	• Protocol type. • The value can be **icmp**, **tcp**, **udp**, **icmpv6** or an IP number. • Constraints: – If the parameter is left blank, all protocols are supported. – When the protocol is **icmpv6**, IP version should be **IPv6**. – When the protocol is **icmp**, IP version should be **IPv4**.
ethertype	String	• IP version. • The value can be **IPv4** or **IPv6**. • If you do not set this parameter, **IPv4** is used by default.
multiport	String	• Port or port range. • The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).
action	String	• Action of the security group rule. • The value can be: – **allow** – **deny** • The default value is **deny**.
priority	Integer	• Rule priority. • The value is from **1** to **100**. The value **1** indicates the highest priority.
remote_group_id	String	• ID of the remote security group, which allows or denies traffic to and from the security group. • Value range: ID of an existing security group • The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_address_group_id**.

Parameter	Type	Description
remote_ip_prefix	String	• Remote IP address. When the direction is **egress**, it is the address of the terminal that accesses the VM. When the direction is **ingress**, it is the address of the VM to be accessed. • The value is an IP address or a CIDR block. • Constraints: – The parameter is mutually exclusive with parameters **remote_group_id** and **remote_address_group_id**. – If this parameter is left blank, the remote IP address is not limited, and the traffic from all remote IP addresses is allowed or rejected.
remote_address_group_id	String	• ID of the remote IP address group. • Value range: ID of an existing IP address group • The parameter is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
created_at	String	• Time when the security group rule is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	• Time when the security group rule is updated • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	• ID of the project to which the security group rule belongs.

Example Response

When the status code is **200**, the response parameters are as follows:

OK

```
{
    "security_group_rule": {
        "id": "f626eb24-d8bd-4d26-ae0b-c16bb65730cb",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "security_group_id": "0552091e-b83a-49dd-88a7-4a5c86fd9ec3",
        "remote_group_id": null,
        "direction": "ingress",
        "protocol": "tcp",
        "description": "security group rule description",
        "created_at": "2020-08-13T07:12:36Z",
        "updated_at": "2020-08-13T07:12:36Z",
```



```
    "ethertype": "IPv4",
    "remote_ip_prefix": "10.10.0.0/16",
    "multiport": "333",
    "remote_address_group_id": null,
    "action": "allow",
    "priority": 1
  },
  "request_id": "034c4840bde0b1263a4b2e66fbd74d5f"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.3.4 Deleting a Security Group Rule

Function

This API is used to delete a security group rule.

URI

DELETE /v3/{project_id}/vpc/security-group-rules/{security_group_rule_id}

Table 5-86 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
security_group_rule_id	Yes	String	Security group rule ID.

Request Parameter

None

Example Request

- Delete a single security group rule.

```
"DELETE https://{Endpoint}/v3/{project_id}/vpc/security-group-rules/01a772b2-463e-47e3-a95d-bac85ee8adc6"
```

Response Parameter

None

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.3.5 Adding Rules to a Specified Security Group

Function

This API is used to add rules to a specified security group.

URI

POST /v3/{project_id}/vpc/security-groups/{security_group_id}/security-group-rules/batch-create

Table 5-87 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
security_group_id	Yes	String	Security Group ID

Request Parameters

Table 5-88 Request body parameters

Parameter	Mandatory	Type	Description
security_group_rules	Yes	Array of **BatchCreateSecurityGroupRulesOption** objects	Request body for batch creating security group rules.
ignore_duplicate	No	Boolean	Specifies whether to ignore duplicate security group rules during creation. The default value is false. Default: **false**

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Whether to only send the check request. The value can be: true: A check request will be sent and no security group rule will be created. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. false (default value): A request will be sent and a security group rule will be created.

Table 5-89 BatchCreateSecurityGroupRulesOption

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
direction	Yes	String	Inbound or outbound direction of a security group rule. The value can be: ingress: inbound direction egress: outbound direction
ethertype	No	String	IP version The value can be IPv4 or IPv6. If you do not set this parameter, IPv4 is used by default.

Parameter	Mandatory	Type	Description
protocol	No	String	Protocol type The value can be icmp, tcp, udp, icmpv6 or an IP number (0 to 255). Constraints: If the parameter is left blank, all protocols are supported.When the protocol is icmpv6, IP version should be IPv6.When the protocol is icmp, IP version should be IPv4.
multiport	No	String	Port or port range The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80). The port is from 1 to 65535.
remote_ip_prefix	No	String	Remote IP address. If direction is set to egress, the parameter specifies the source IP address. If direction is set to ingress, the parameter specifies the destination IP address. The value is an IP address or a CIDR block. Constraints:The parameter is mutually exclusive with parameters remote_group_id and remote_address_group_id.If this parameter is left blank, the remote IP address is not limited, and the traffic from all remote IP addresses is allowed or rejected.

Parameter	Mandatory	Type	Description
remote_group_id	No	String	ID of the remote security group, which allows or denies traffic to and from the security group. Value range: ID of an existing security group The parameter is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_address_group_id	No	String	ID of the remote IP address group. Value range: ID of an existing IP address group The parameter is mutually exclusive with parameters remote_ip_prefix and remote_group_id.
action	No	String	Action of the security group rule. The value can be:allow, deny. The default value is allow.
priority	No	String	Rule priority in a security group. The value is from 1 to 100. The value 1 indicates the highest priority. The default value is 1.

Response Parameters

Status code: 201

Table 5-90 Response body parameters

Parameter	Type	Description
security_group_rules	Array of **SecurityGroupRule** objects	Response body for batch creating security group rules.
request_id	String	Request ID.

Table 5-91 SecurityGroupRule

Parameter	Type	Description
id	String	Security group rule ID, which uniquely identifies the security group ruleThe value is in UUID format with hyphens (-).
description	String	Provides supplementary information about the security group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_group_id	String	ID of the security group to which the security group rule belongs.
direction	String	Inbound or outbound direction of a security group rule. The value can be: ingress: inbound direction egress: outbound direction
protocol	String	Protocol type The value can be icmp, tcp, udp, icmpv6 or an IP number. Constraints: If the parameter is left blank, all protocols are supported. When the protocol is icmpv6, IP version should be IPv6. When the protocol is icmp, IP version should be IPv4.
ethertype	String	IP version The value can be IPv4 or IPv6. If you do not set this parameter, IPv4 is used by default. Default: **IPv4**
multiport	String	Port or port range The value can be a single port (80), a port range (1-30), or inconsecutive ports separated by commas (22,3389,80).
action	String	Action of the security group rule. The value can be: allow, deny. The default value is deny.

Parameter	Type	Description
priority	Integer	Rule priority. The value is from 1 to 100. The value 1 indicates the highest priority.
remote_group_id	String	ID of the remote security group, which allows or denies traffic to and from the security group. Value range: ID of an existing security group. The parameter is mutually exclusive with parameters remote_ip_prefix and remote_address_group_id.
remote_ip_prefix	String	Remote IP address. If direction is set to egress, the parameter specifies the source IP address. If direction is set to ingress, the parameter specifies the destination IP address. The value is an IP address or a CIDR block. Constraints: The parameter is mutually exclusive with parameters remote_group_id and remote_address_group_id. If this parameter is left blank, the remote IP address is not limited, and the traffic from all remote IP addresses is allowed or rejected.
remote_address_group_id	String	ID of the remote IP address group. Value range: ID of an existing IP address group The parameter is mutually exclusive with parameters remote_ip_prefix and remote_group_id.
created_at	String	Time when the security group rule is created. UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	Time when the security group rule is updated. UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
project_id	String	ID of the project to which the security group rule belongs.

Example Requests

Adding two inbound rules to the security group whose ID is **15457509-18f9-4387-bae6-d4ed1898b301** with duplicate rules ignored

```
POST https://{Endpoint}/v3/{project_id}/vpc/security-groups/15457509-18f9-4387-bae6-d4ed1898b301/security-group-rules/batch-create
```



```
{
  "ignore_duplicate" : true,
  "security_group_rules" : [ {
    "direction" : "ingress",
    "description" : "",
    "protocol" : "tcp",
    "action" : "allow",
    "priority" : 1,
    "ethertype" : "IPv4",
    "multiport" : "22",
    "remote_ip_prefix" : "117.78.12.122/32"
  }, {
    "direction" : "ingress",
    "description" : "",
    "protocol" : "tcp",
    "action" : "allow",
    "priority" : 1,
    "ethertype" : "IPv4",
    "multiport" : "22",
    "remote_ip_prefix" : "117.78.12.122/32"
  } ]
}
```

Example Responses

Status code: 201

Created

```
{
  "security_group_rules" : [ {
    "id" : "abef369b-d646-4b8a-9f44-fcd248a6c421",
    "project_id" : "5f6387106c2048b589b369d96c2f23a2",
    "security_group_id" : "15457509-18f9-4387-bae6-d4ed1898b301",
    "direction" : "ingress",
    "protocol" : "tcp",
    "description" : "",
    "created_at" : "2023-04-28T04:08:52.000+00:00",
    "updated_at" : "2023-04-28T04:08:52.000+00:00",
    "ethertype" : "IPv4",
    "remote_ip_prefix" : "117.78.12.122/32",
    "multiport" : 22,
    "action" : "allow",
    "priority" : 1
  } ],
  "request_id" : "f1ae2c6f9e94babf077cd3b3e1570c81"
}
```

Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

5.4 IP Address Group

5.4.1 Creating an IP Address Group

Function

This API is used to create an IP address group.

Constraints

The default IP address group quota for each account is 50.

URI

POST /v3/{project_id}/vpc/address-groups

Table 5-92 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameter

Table 5-93 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Whether to only send the check request. • The value can be: – **true**: A check request will be sent and no IP address group will be created. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. – **false** (default value): A request will be sent and an IP address group will be created.
address_group	Yes	**CreateAddressGroupOption** object	Request body for creating an IP address group.

Table 5-94 CreateAddressGroupOption

Parameter	Mandatory	Type	Description
name	Yes	String	• IP address group name. • The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	• Provides supplementary information about an IP address group. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Parameter	Mandatory	Type	Description
ip_version	Yes	Integer	• The IP version of the address group. • The value can be: – **4**: IPv4 address group. – **6**: IPv6 address group.
max_capacity	No	Integer	• Maximum number of IP addresses or IP address ranges in an IP address group. • The value can be from **0** to **20**. • The default value is **20**.
ip_set	No	Array of strings	• IP address sets in an IP address group. • The value can be a single IP address, IP address range, or CIDR block. • The default maximum number of IP address sets, including IP addresses, IP address ranges, and CIDR blocks, in an IP address group is 20.
enterprise_project_id	No	String	• Enterprise project ID. This is the ID of enterprise project bound to the IP address group when you create the group. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. • Default value: **0** • This parameter is available in CN South-Shenzhen, CN Southwest-Guiyang1, CN South-Guangzhou, AP-Singapore, CN East-Shanghai1, and CN North-Beijing4.
ip_extra_set	No	Array of **IpExtraSetOption** objects	• IP addresses and their remarks in an IP address group. • The default quota is 20. Either this parameter or **ip_set** must be specified.

Table 5-95 IpExtraSetOption

Parameter	Mandatory	Type	Description
ip	Yes	String	• An IP address, IP address range, or CIDR block. Both IPv4 and IPv6 are supported.
remarks	No	String	• Provides supplementary information about the IP address, IP address range, or CIDR block. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Example Request

- Create an IP address group named **AutoTester746010.580123789**, set the IP version to IPv4, and the IP set to 192.168.3.2, 192.168.3.40, 192.168.3.20-192.168.3.100, and 192.168.5.0/24.

```
POST https://{{endpoint}}/v3/b2782e6708b8475c993e6064bc456bf8/vpc/address-groups

{
    "address_group": {
        "ip_version": 4,
        "name": "AutoTester746010.580123789",
        "ip_set": [
            "192.168.3.2",
            "192.168.3.40",
            "192.168.3.20-192.168.3.100",
            "192.168.5.0/24"
        ],
        "description": "test",
        "max_capacity": 20,
        "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2"
    }
}
```

Response Parameter

When the status code is **201**, the response parameters are as follows:

Table 5-96 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
address_group	**AddressGroup** object	Response body for creating an IP address group.

Table 5-97 AddressGroup

Parameter	Type	Description
id	String	• IP address group ID that uniquely identifies the IP address group. • The value is a string in UUID format.
name	String	• IP address group name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about an IP address group. • The value can contain up to 255 characters. • The value cannot contain angle brackets (< or >).
ip_set	Array of strings	• IP address sets in an IP address group. • The value can be a single IP address, IP address range, or CIDR block. • The default maximum number of IP address sets, including IP addresses, IP address ranges, and CIDR blocks, in an IP address group is 20.
ip_version	Integer	• Whether it is an IPv4 or IPv6 address group. • The value can be: – **4**: IPv4 address group. – **6**: IPv6 address group.
created_at	String	• Time (UTC) when the IP address group is created. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
updated_at	String	• Time (UTC) when the IP address group was last updated. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
tenant_id	String	• ID of the project to which the IP address group belongs.
max_capacity	Integer	• Maximum number of IP addresses or IP address ranges in an IP address group. • The value can be from **0** to **20**. • The default value is **20**.

Parameter	Type	Description
enterprise_project_id	String	• Enterprise project ID. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. • Maximum length: **36** • This parameter is available in CN South-Shenzhen, CN Southwest-Guiyang1, CN South-Guangzhou, AP-Singapore, CN East-Shanghai1, and CN North-Beijing4.
tags	Array of **ResourceTag** objects	IP address group tags.
status	String	• IP address group status. • Value range (Default value: **NORMAL**) – **NORMAL** – **UPDATING** – **UPDATE_FAILED** • An IP address group in the **UPDATING** state cannot be updated again.
status_message	String	• IP address group status details.
ip_extra_set	Array of **IpExtraSetRespOption** objects	• IP address sets and their remarks in an IP address group.

Table 5-98 ResourceTag

Parameter	Type	Description
key	String	• Tag key. • Tag keys must be unique for each resource. • Minimum length: **1** • Maximum length: **128**
value	String	• Tag value. • Maximum length: **255**

Table 5-99 IpExtraSetRespOption

Parameter	Type	Description
ip	String	• An IP address, IP address range, or CIDR block. Both IPv4 and IPv6 are supported.
remarks	String	• Provides supplementary information about the IP address, IP address range, or CIDR block. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Example Response

When the status code is **201**, the response parameters are as follows:

Normal response for the POST operation of the API for creating an IP address group

```
{
   "address_group": {
      "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
      "name": "AutoTester746010.580123789",
      "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
      "ip_version": 4,
      "ip_set": [
         "192.168.5.0/24",
         "192.168.3.20-192.168.3.100",
         "192.168.3.40",
         "192.168.3.2"
      ],
      "ip_extra_set": [{
      "ip": "192.168.5.0/24",
      "remarks": null
   },
   {
         "ip": "192.168.3.20-192.168.3.100",
      "remarks": null
   },
   {
      "ip": "192.168.3.40",
      "remarks": null
   },
   {
      "ip": "192.168.3.2",
      "remarks": null
   }],
      "created_at": "2019-06-28T02:06:38",
      "updated_at": "2019-06-28T02:06:38",
      "description": "test",
      "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
      "tags": [],
      "max_capacity": 20,
      "status": "NORMAL",
      "status_message": ""
   },
   "request_id": "f568db7a-2675-4271-8747-3e3f1c6381ba"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.4.2 Querying IP Address Groups

Function

This API is used to query IP address groups based on filter criteria.

URI

GET /v3/{project_id}/vpc/address-groups

Table 5-100 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Table 5-101 Query parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records displayed on each page. Value range: 0 to 2000
enterprise_project_id	No	String	Enterprise project ID. This field can be used to filter the IP address groups of an enterprise project. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. To obtain the IP address groups bound to all enterprise projects of the user, set **all_granted_eps**. Maximum length: **36** This parameter is available in CN South-Shenzhen, CN Southwest-Guiyang1, CN South-Guangzhou, and AP-Singapore.

Parameter	Mandatory	Type	Description
marker	No	String	Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.
id	No	Array of strings	Unique ID of an IP address group, which can be used to filter the IP address group.
name	No	Array of strings	Name of an IP address group, which can be used to filter the IP address group.
ip_version	No	Integer	Version of IP addresses in an IP address group. The value can be **4** or **6**.
description	No	Array of strings	Provides supplementary information about an IP address group, which can be used to filter the IP address group.

Request Parameter

None

Example Request

- Query IP address groups based on combined filtering criteria

```
"GET https://{{endpoint}}/v3/b2782e6708b8475c993e6064bc456bf8/vpc/address-groups?name=vkvgykvsvhjaaaa1&description=xxxxxxxxxx&ip_version=4"
```

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-102 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
address_groups	Array of **AddressGroup** objects	Response body of IP address groups
page_info	**PageInfo** object	Pagination information

Table 5-103 AddressGroup

Parameter	Type	Description
id	String	• IP address group ID that uniquely identifies the IP address group. • The value is a string in UUID format.
name	String	• IP address group name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about an IP address group. • The value can contain up to 255 characters. • The value cannot contain angle brackets (< or >).
ip_set	Array of strings	• IP address sets in an IP address group. • The value can be a single IP address, IP address range, or CIDR block. • The default maximum number of IP address sets, including IP addresses, IP address ranges, and CIDR blocks, in an IP address group is 20.
ip_version	Integer	• Whether it is an IPv4 or IPv6 address group. • The value can be: – **4**: IPv4 address group. – **6**: IPv6 address group.
created_at	String	• Time (UTC) when the IP address group is created. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
updated_at	String	• Time (UTC) when the IP address group was last updated. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
tenant_id	String	• ID of the project to which the IP address group belongs.
max_capacity	Integer	• Maximum number of IP addresses or IP address ranges in an IP address group. • The value can be from **0** to **20**. • The default value is **20**.

Parameter	Type	Description
enterprise_project_id	String	• Enterprise project ID. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. • Maximum length: **36** • This parameter is available in CN South-Shenzhen, CN Southwest-Guiyang1, CN South-Guangzhou, AP-Singapore, CN East-Shanghai1, and CN North-Beijing4.
tags	Array of **ResourceTag** objects	IP address group tags.
status	String	• IP address group status. • Value range (Default value: **NORMAL**) – **NORMAL** – **UPDATING** – **UPDATE_FAILED** • An IP address group in the **UPDATING** state cannot be updated again.
status_message	String	• IP address group status details.
ip_extra_set	Array of **IpExtraSetRespOption** objects	• IP address sets and their remarks in an IP address group.

Table 5-104 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page
current_count	Integer	Total number of records on the current page
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Table 5-105 ResourceTag

Parameter	Type	Description
key	String	Tag key. Each key value of a resource must be unique. Minimum length: **1** Maximum length: **128**
value	String	Tag value Maximum length: **255**

Table 5-106 IpExtraSetRespOption

Parameter	Type	Description
ip	String	An IP address, IP address range, or CIDR block. Both IPv4 and IPv6 are supported.
remarks	String	Provides supplementary information about the IP address, IP address range, or CIDR block. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Example Response

When the status code is **200**, the response parameters are as follows:

Normal response for the GET operation of the API for querying an IP address group

```
{
   "address_groups": [
      {
         "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
         "name": "AutoTester746010.580123789",
         "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
         "ip_version": 4,
         "ip_set": [
            "192.168.5.0/24",
            "192.168.3.20-192.168.3.100",
            "192.168.3.40",
            "192.168.3.2"
         ],
         "ip_extra_set": [{
         "ip": "192.168.5.0/24",
         "remarks": null
      },
      {
            "ip": "192.168.3.20-192.168.3.100",
         "remarks": null
      },
      {
         "ip": "192.168.3.40",
         "remarks": null
      },
```



```
        {
            "ip": "192.168.3.2",
            "remarks": null
        }],
            "created_at": "2019-06-28T02:06:38",
            "updated_at": "2019-06-28T02:06:38",
            "description": "test",
            "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
            "tags": [],
            "max_capacity": 20,
            "status": "NORMAL",
            "status_message": ""
        }
    ],
    "page_info": {
        "previous_marker": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
        "current_count": 1
    },
    "request_id": "e51fa17c-3259-4122-afb1-9c03d4ef5408"
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.4.3 Querying Details of an IP Address Group

Function

This API is used to query details of an IP address group.

URI

GET /v3/{project_id}/vpc/address-groups/{address_group_id}

Table 5-107 Parameter description

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	IP address group ID that uniquely identifies the IP address group.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameter

None

Example Request

- Querying details of an IP address group

```
"GET https://{Endpoint}/v3/2bc7a67b35a64a79ad1d3bb8b5f61fc9/vpc/address-groups/dd18a501-fcd5-4adc-acfe-b0e2384baf08"
```

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-108 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
address_group	**AddressGroup** object	Response body of querying an IP address group

Table 5-109 AddressGroup

Parameter	Type	Description
id	String	• IP address group ID that uniquely identifies the IP address group. • The value is a string in UUID format.
name	String	• IP address group name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about an IP address group. • The value can contain up to 255 characters. • The value cannot contain angle brackets (< or >).
ip_set	Array of strings	• IP address sets in an IP address group. • The value can be a single IP address, IP address range, or CIDR block. • The default maximum number of IP address sets, including IP addresses, IP address ranges, and CIDR blocks, in an IP address group is 20.
ip_version	Integer	• Whether it is an IPv4 or IPv6 address group. • The value can be: – **4**: IPv4 address group. – **6**: IPv6 address group.

Parameter	Type	Description
created_at	String	• Time (UTC) when the IP address group is created. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
updated_at	String	• Time (UTC) when the IP address group was last updated. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
tenant_id	String	• ID of the project to which the IP address group belongs.
max_capacity	Integer	• Maximum number of IP addresses or IP address ranges in an IP address group. • The value can be from **0** to **20**. • The default value is **20**.
enterprise_project_id	String	• Enterprise project ID. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. • Maximum length: **36** • This parameter is available in CN South-Shenzhen, CN Southwest-Guiyang1, CN South-Guangzhou, AP-Singapore, CN East-Shanghai1, and CN North-Beijing4.
tags	Array of **ResourceTag** objects	IP address group tags.
status	String	• IP address group status. • Value range (Default value: **NORMAL**) – **NORMAL** – **UPDATING** – **UPDATE_FAILED** • An IP address group in the **UPDATING** state cannot be updated again.
status_message	String	• IP address group status details.
ip_extra_set	Array of **IpExtraSetRespOption** objects	• IP address sets and their remarks in an IP address group.

Table 5-110 ResourceTag

Parameter	Type	Description
key	String	Tag key. Each key value of a resource must be unique. Minimum length: **1** Maximum length: **128**
value	String	Tag value Maximum length: **255**

Table 5-111 IpExtraSetOption

Parameter	Mandatory	Type	Description
ip	Yes	String	An IP address, IP address range, or CIDR block. Both IPv4 and IPv6 are supported.
remarks	No	String	Provides supplementary information about the IP address, IP address range, or CIDR block. The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Example Response

When the status code is **200**, the response parameters are as follows:

Normal response for the GET operation of the API for querying an IP address group

```
{
   "address_group": {
      "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
      "name": "AutoTester746010.580123789",
      "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
      "ip_version": 4,
      "ip_set": [
         "192.168.5.0/24",
         "192.168.3.20-192.168.3.100",
         "192.168.3.40",
         "192.168.3.2"
      ],
      "ip_extra_set": [{
      "ip": "192.168.5.0/24",
      "remarks": null
   },
   {
         "ip": "192.168.3.20-192.168.3.100",
      "remarks": null
   },
   {
```



```
        "ip": "192.168.3.40",
        "remarks": null
    },
    {
        "ip": "192.168.3.2",
        "remarks": null
    }],
        "created_at": "2019-06-28T02:06:38",
        "updated_at": "2019-06-28T02:06:38",
        "description": "10.10.4.0/23",
        "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
        "tags": [],
        "max_capacity": 20,
        "status": "NORMAL",
        "status_message": ""
    },
    "request_id": "ce6c359b-9002-41e5-a0b1-232759bd6637"
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.4.4 Updating an IP Address Group

Function

This API is used to update an IP address group.

URI

PUT /v3/{project_id}/vpc/address-groups/{address_group_id}

Table 5-112 Parameter description

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	IP address group ID that uniquely identifies the IP address group.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameter

Table 5-113 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Whether to only send the check request. • The value can be: – **true**: A check request will be sent and no IP address group will be updated. Check items include mandatory parameters, request format, and permission verification. If the check fails, an error will be returned. If the check succeeds, response code 202 will be returned. – **false** (default value): A request will be sent and an IP address group will be updated.
address_group	Yes	**UpdateAddressGroupOption** object	Request body for updating an IP address group.

Table 5-114 UpdateAddressGroupOption

Parameter	Mandatory	Type	Description
name	No	String	• IP address group name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	• Provides supplementary information about the IP address group. • The value can contain up to 255 characters. • The value cannot contain angle brackets (< or >).

Parameter	Mandatory	Type	Description
ip_set	No	Array of strings	• IP address sets in an IP address group. • The value can be a single IP address, IP address range, or CIDR block. • The default maximum number of IP address sets, including IP addresses, IP address ranges, and CIDR blocks, in an IP address group is 20.
max_capacity	No	Integer	• Maximum number of IP addresses or IP address ranges in an IP address group. • The value can be from **0** to **20**.
ip_extra_set	No	Array of **IpExtraSetOption** objects	• IP addresses and their remarks in an IP address group. • The default quota is 20. Either this parameter or **ip_set** must be specified.

Table 5-115 IpExtraSetOption

Parameter	Mandatory	Type	Description
ip	Yes	String	• An IP address, IP address range, or CIDR block. Both IPv4 and IPv6 are supported.
remarks	No	String	• Provides supplementary information about the IP address, IP address range, or CIDR block. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Example Request

- Change the name, IP set, and description of the IP address group whose ID is dd18a501-fcd5-4adc-acfe-b0e2384baf08.

```
"PUT https://{endpoint}/v3/b2782e6708b8475c993e6064bc456bf8/vpc/address-groups/dd18a501-fcd5-4adc-acfe-b0e2384baf08"

{
    "address_group": {
```



```
    "name": "vkvgykvsvhjaaaa1",
    "ip_set": [
      "192.168.3.2",
      "192.168.3.43",
      "192.168.3.20-192.168.3.100",
      "192.168.5.0/24"
    ],
    "description": "xxxxxxxxxx"
  }
}
```

Response Parameter

When the status code is **200**, the response parameters are as follows:

Table 5-116 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
address_group	**AddressGroup** object	Response body for updating an IP address group

Table 5-117 AddressGroup

Parameter	Type	Description
id	String	• IP address group ID that uniquely identifies the IP address group. • The value is a string in UUID format.
name	String	• IP address group name. • The value can contain up to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	• Provides supplementary information about an IP address group. • The value can contain up to 255 characters. • The value cannot contain angle brackets (< or >).
ip_set	Array of strings	• IP address sets in an IP address group. • The value can be a single IP address, IP address range, or CIDR block. • The default maximum number of IP address sets, including IP addresses, IP address ranges, and CIDR blocks, in an IP address group is 20.

Parameter	Type	Description
ip_version	Integer	• Whether it is an IPv4 or IPv6 address group. • The value can be: – **4**: IPv4 address group. – **6**: IPv6 address group.
created_at	String	• Time (UTC) when the IP address group is created. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
updated_at	String	• Time (UTC) when the IP address group was last updated. • The value must be the UTC time in the format of yyyy-MM-ddTHH:mmss.
tenant_id	String	• ID of the project to which the IP address group belongs.
max_capacity	Integer	• Maximum number of IP addresses or IP address ranges in an IP address group. • The value can be from **0** to **20**. • The default value is **20**.
enterprise_project_id	String	• Enterprise project ID. • The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. • Maximum length: **36** • This parameter is available in CN South-Shenzhen, CN Southwest-Guiyang1, CN South-Guangzhou, AP-Singapore, CN East-Shanghai1, and CN North-Beijing4.
tags	Array of **ResourceTag** objects	IP address group tags.
status	String	• IP address group status. • Value range (Default value: **NORMAL**) – **NORMAL** – **UPDATING** – **UPDATE_FAILED** • An IP address group in the **UPDATING** state cannot be updated again.
status_message	String	• IP address group status details.

Parameter	Type	Description
ip_extra_set	Array of **IpExtraSetRespOption** objects	• IP address sets and their remarks in an IP address group.

Table 5-118 ResourceTag

Parameter	Type	Description
key	String	• Tag key • Tag keys must be unique for each resource. • Minimum length: **1** • Maximum length: **128**
value	String	• Tag value • Maximum length: **255**

Table 5-119 IpExtraSetRespOption

Parameter	Type	Description
ip	String	• An IP address, IP address range, or CIDR block. Both IPv4 and IPv6 are supported.
remarks	String	• Provides supplementary information about the IP address, IP address range, or CIDR block. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Example Response

When the status code is **200**, the response parameters are as follows:

Normal response for the PUT operation of the API for updating an IP address group

```
{
    "address_group": {
        "id": "dd18a501-fcd5-4adc-acfe-b0e2384baf08",
        "name": "vkvgykvsvhjaaaa1",
        "tenant_id": "b2782e6708b8475c993e6064bc456bf8",
        "ip_version": 4,
        "ip_set": [
            "192.168.5.0/24",
            "192.168.3.20-192.168.3.100",
            "192.168.3.43",
            "192.168.3.2"
        ],
        "ip_extra_set": [{
```



```
      "ip": "192.168.5.0/24",
      "remarks": null
    },
    {
        "ip": "192.168.3.20-192.168.3.100",
      "remarks": null
    },
    {
      "ip": "192.168.3.43",
      "remarks": null
    },
    {
      "ip": "192.168.3.2",
      "remarks": null
    }],
      "created_at": "2019-06-28T02:06:38",
      "updated_at": "2019-06-28T02:14:01",
      "description": "xxxxxxxxxx",
      "enterprise_project_id": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
      "tags": [],
      "max_capacity": 20,
      "status": "NORMAL",
      "status_message": ""
    },
    "request_id": "5bbd1640-fa68-4362-9a5c-30c4809958e0"
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.4.5 Deleting an IP Address Group

Function

This API is used to delete an IP address group. Before deleting an IP address group, ensure that no resource is using this group.

URI

DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}

Table 5-120 Parameter description

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	IP address group ID that uniquely identifies the IP address group.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameter

None

Example Request

- Deleting an IP address group
  ```
  "DELETE https://{{endpoint}}/v3/{{tenant_id}}/vpc/address-groups/dd18a501-fcd5-4adc-acfe-b0e2384baf08"
  ```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.4.6 Forcibly Deleting an IP Address Group

Function

This API is used to forcibly delete an IP address group. If the IP address group to be deleted has associated security group rules, the IP address group and its associated rules will be deleted together.

URI

DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}/force

Table 5-121 URI parameters

Parameter	Mandatory	Type	Description
address_group_id	Yes	String	ID of the IP address group to be deleted. It uniquely identifies an IP address group.
project_id	Yes	String	Project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Request Parameter

None

Example Request

- Forcibly deleting an IP address group
  "DELETE https://{{endpoint}}/v3/{{tenant_id}}/vpc/address-groups/dd18a501-fcd5-4adc-acfe-b0e2384baf08/force"

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

5.5 Supplementary Network Interfaces

NOTE

Supplementary network interfaces are now available only in CN North-Beijing4, CN North-Beijing2, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Singapore, AP-Jakarta, LA-Mexico City2, and TR-Istanbul.

5.5.1 Creating a Supplementary Network Interface

Function

This API is used to create a supplementary network interface.

URI

POST /v3/{project_id}/vpc/sub-network-interfaces

Table 5-122 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 5-123 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Whether to only send the check request. • The value can be: – **true**: A check request will be sent and no supplementary network interface will be created. Check items include mandatory parameters, request format, and permission verification. If the check fails, the system returns an error. If the check succeeds, response code 202 will be returned. – **false** (default value): A request will be sent and a supplementary network interface will be created.
sub_network_interface	Yes	**CreateSubNetworkInterfaceOption** object	Request body for creating a supplementary network interface.

Table 5-124 CreateSubNetworkInterfaceOption

Parameter	Mandatory	Type	Description
virsubnet_id	Yes	String	• Virtual subnet ID, also the subnet ID, which is the same as the network ID displayed on the subnet summary page on the console. • The value must be in standard UUID format.
vlan_id	No	String	• VLAN ID of the supplementary network interface. • The value can be from 1 to 4094. • Each supplementary network interface of an elastic network interface has a unique VLAN ID.

Parameter	Mandatory	Type	Description
parent_id	Yes	String	• ID of the elastic network interface. • The value must be in standard UUID format. • The value must be an existing port ID.
description	No	String	• Description of the supplementary network interface. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
ipv6_enable	No	Boolean	• Whether to enable IPv6 for the supplementary network interface. • The value can be: – **true**: Enable – **false**: Disable • The default value is **false**.
private_ip_address	No	String	• Private IPv4 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
ipv6_ip_address	No	String	• Private IPv6 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
security_groups	No	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"] • The default value is the default security group.
project_id	No	String	• Project ID of the supplementary network interface. • The value must be in standard UUID format. • Only administrators have permissions to specify project IDs.

Response Parameters

When the status code is **201**, the response parameters are as follows:

Table 5-125 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
sub_network_interface	**SubNetworkInterface** object	Response body of a supplementary network interface.

Table 5-126 SubNetworkInterface

Parameter	Type	Description
id	String	• Unique identifier of the supplementary network interface. • The value is in UUID format with hyphens (-).
virsubnet_id	String	• Virtual subnet ID, also the subnet ID, which is the same as the network ID displayed on the subnet summary page on the console. • The value must be in standard UUID format.
private_ip_address	String	• Private IPv4 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
ipv6_ip_address	String	• Private IPv6 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
mac_address	String	• MAC address of the supplementary network interface. • The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	• Device ID. • The value must be in standard UUID format.
parent_id	String	• ID of the elastic network interface. • The value must be in standard UUID format.

Parameter	Type	Description
description	String	• Description of the supplementary network interface. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	• VPC ID of the supplementary network interface. • The value must be in standard UUID format.
vlan_id	Integer	• VLAN ID of the supplementary network interface. • The value can be from 1 to 4094. • Each supplementary network interface of an elastic network interface has a unique VLAN ID.
security_enabled	Boolean	• Whether the security option is enabled for the supplementary network interface. If the option is not enabled, the security group does not take effect.
security_groups	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"] • The default value is the default security group.
tags	Array of strings	• Tags of the supplementary network interface.
project_id	String	• Project ID of the supplementary network interface.
created_at	String	• The time when the supplementary network interface is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Request

Create a supplementary network interface. Set its virtual subnet ID to 08278e6c-61ca-46c1-9fc3-0d4f6c12f193, elastic network interface ID to 637748df-2986-4350-8303-95d259580fb3, and associated security group to 6727c950-9f01-47a2-a7aa-7d3686c4c95b.

```
POST https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces

{
  "sub_network_interface" : {
    "virsubnet_id" : "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
    "parent_id" : "637748df-2986-4350-8303-95d259580fb3",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ]
```



```
  }
}
```

Example Response

When the status code is **201**, the response parameters are as follows:

Created

```
{
  "sub_network_interface" : {
    "id" : "2be868f2-f7c9-48db-abc0-eea0b9105b0d",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
    "private_ip_address" : "10.0.0.225",
    "ipv6_ip_address" : null,
    "mac_address" : "fa:16:3e:48:f8:6f",
    "parent_device_id" : "1ab01f1d-4ef7-4d83-82be-802b3aca0223",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : "63b97e6b-3598-430f-9eb8-1caf06937be8",
    "description" : null,
    "parent_id" : "637748df-2986-4350-8303-95d259580fb3",
    "vlan_id" : 2787,
    "tags" : [ ],
    "created_at" : "2020-05-19T01:16:25Z"
  },
  "request_id" : "ceb6273e-1ec9-4168-ac11-3dfeaacfc889"
}
```

Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

5.5.2 Creating Supplementary Network Interfaces in Batches

Function

This API is used to create supplementary network interfaces in batches.

URI

POST /v3/{project_id}/vpc/sub-network-interfaces/batch-create

Table 5-127 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 5-128 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Whether to only send the check request. • The value can be: – **true**: A check request will be sent and no supplementary network interface will be created. Check items include mandatory parameters, request format, and permission verification. If the check fails, the system returns an error. If the check succeeds, response code 202 will be returned. – **false** (default value): A request will be sent and a supplementary network interface will be created.
sub_network_interface	Yes	**BatchCreateSubNetworkInterfaceOption** object	Request body for creating a supplementary network interface.
count	Yes	Integer	• Number of supplementary network interfaces to be created in batches. • Minimum value: **1** • Maximum value: **20**

Table 5-129 BatchCreateSubNetworkInterfaceOption

Parameter	Mandatory	Type	Description
virsubnet_id	Yes	String	• Virtual subnet ID, which is the subnet ID and is the same as the network ID displayed on the subnet summary page on the console. • The value must be in standard UUID format.
parent_id	Yes	String	• ID of the elastic network interface • The value must be in standard UUID format. • The value must be an existing port ID.
security_groups	No	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"] • The default value is the default security group.
description	No	String	• Description of the supplementary network interface • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
ipv6_enable	No	Boolean	• Whether to enable IPv6 for the supplementary network interface • The value can be: – **true**: Enable – **false**: Disable • The default value is **false**.
project_id	No	String	• Project ID of the supplementary network interface • The value must be in standard UUID format. • Only administrators have permissions to specify project IDs.

Response Parameters

When the status code is **201**, the response parameters are as follows:

Table 5-130 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
sub_network_interfaces	Array of **SubNetworkInterface** objects	Response body for creating supplementary network interfaces in batches.

Table 5-131 SubNetworkInterface

Parameter	Type	Description
id	String	• Unique identifier of the supplementary network interface. • The value is in UUID format with hyphens (-).
virsubnet_id	String	• Virtual subnet ID, also the subnet ID, which is the same as the network ID displayed on the subnet summary page on the console. • The value must be in standard UUID format.
private_ip_address	String	• Private IPv4 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
ipv6_ip_address	String	• Private IPv6 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
mac_address	String	• MAC address of the supplementary network interface. • The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	• Device ID. • The value must be in standard UUID format.
parent_id	String	• ID of the elastic network interface. • The value must be in standard UUID format.

Parameter	Type	Description
description	String	• Description of the supplementary network interface. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	• VPC ID of the supplementary network interface. • The value must be in standard UUID format.
vlan_id	Integer	• VLAN ID of the supplementary network interface. • The value can be from 1 to 4094. • Each supplementary network interface of an elastic network interface has a unique VLAN ID.
security_enabled	Boolean	• Whether the security option is enabled for the supplementary network interface. If the option is not enabled, the security group does not take effect.
security_groups	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"] • The default value is the default security group.
tags	Array of strings	• Tags of the supplementary network interface.
project_id	String	• Project ID of the supplementary network interface.
created_at	String	• The time when the supplementary network interface is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Request

Create three supplementary network interfaces in batches. Set the virtual subnet ID to 115b5a84-31dc-4b1e-8de9-bf5a75d2c566, elastic network interface ID to 8b6c46f1-c68d-4bba-a922-2d97da185af5, and associated security group to 6727c950-9f01-47a2-a7aa-7d3686c4c95b.

```
POST https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces/batch-create

{
  "sub_network_interface" : {
    "virsubnet_id" : "115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "parent_id" : "8b6c46f1-c68d-4bba-a922-2d97da185af5"
```



```
  },
  "count" : 3
}
```

Example Response

When the status code is **201**, the response parameters are as follows:

Created

```
{
  "sub_network_interfaces" : [ {
    "id" : "d1f8094c-bb3d-43c5-b625-52dd43eab451",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
    "private_ip_address" : "192.168.6.245",
    "ipv6_ip_address" : "2001:db8:a583:5d:11e8:b908:4fe6:9802",
    "mac_address" : "fa:16:3e:97:1f:f5",
    "parent_device_id" : "11185aa2-4e08-4d9e-87ed-84817280eaa7",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : null,
    "description" : "",
    "parent_id" : "8b6c46f1-c68d-4bba-a922-2d97da185af5",
    "vlan_id" : 41,
    "tags" : [ ]
  }, {
    "id" : "0dce57ab-00de-443b-a7fe-e8ff68bd95bc",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
    "private_ip_address" : "192.168.6.75",
    "ipv6_ip_address" : "2001:db8:a583:5d:6c22:8ea2:c061:a802",
    "mac_address" : "fa:16:3e:5a:61:84",
    "parent_device_id" : "11185aa2-4e08-4d9e-87ed-84817280eaa7",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : null,
    "description" : "",
    "parent_id" : "8b6c46f1-c68d-4bba-a922-2d97da185af5",
    "vlan_id" : 42,
    "tags" : [ ]
  }, {
    "id" : "1eca03ee-c0f1-4434-9c4c-87fe4426718c",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "115b5a84-31dc-4b1e-8de9-bf5a75d2c566",
    "private_ip_address" : "192.168.6.194",
    "ipv6_ip_address" : "2001:db8:a583:5d:2b45:a3ae:17db:ec02",
    "mac_address" : "fa:16:3e:b8:ec:6d",
    "parent_device_id" : "11185aa2-4e08-4d9e-87ed-84817280eaa7",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : null,
    "description" : "",
    "parent_id" : "8b6c46f1-c68d-4bba-a922-2d97da185af5",
    "vlan_id" : 43,
    "tags" : [ ]
  } ],
  "request_id" : "344544c1-d053-4ad3-b673-900a0e01db7e"
}
```

Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

5.5.3 Querying Supplementary Network Interfaces

Function

This API is used to query supplementary network interfaces. A maximum of 2,000 records can be returned for each query.

URI

GET /v3/{project_id}/vpc/sub-network-interfaces

Table 5-132 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 5-133 Query parameters

Parameter	Mandatory	Type	Description
id	No	ARRAY	• ID of the supplementary network interface. Multiple IDs can be specified for filtering. • This parameter can be used to filter supplementary network interfaces.
description	No	ARRAY	• Description of the supplementary network interface. Multiple descriptions can be specified for filtering. • This parameter can be used to filter supplementary network interfaces.
limit	No	Integer	Number of records returned on each page.

Parameter	Mandatory	Type	Description
mac_address	No	ARRAY	• MAC address of the supplementary network interface. Multiple MAC addresses can be specified for filtering. • This parameter can be used to precisely filter supplementary network interfaces.
marker	No	String	Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.
parent_id	No	ARRAY	• ID of elastic network interface that the supplementary network interface is attached to. Multiple IDs can be specified for filtering. • This parameter can be used to filter supplementary network interfaces of one or more elastic network interfaces.
private_ip_address	No	ARRAY	• Private IPv4 address of the supplementary network interface. Multiple private IPv4 addresses can be specified for filtering. • This parameter can be used to filter supplementary network interfaces.
virsubnet_id	No	ARRAY	• Virtual subnet ID of the supplementary network interface. Multiple IDs can be specified for filtering. • This parameter can be used to filter supplementary network interfaces in one or more virtual subnets.
vpc_id	No	ARRAY	• VPC ID of the supplementary network interface. Multiple IDs can be specified for filtering. • This field can be used to filter supplementary network interfaces in one or more VPCs.

Request Parameters

None

Response Parameters

When the status code is **200**, the response parameters are as follows:

Table 5-134 Response body parameters

Parameter	Type	Description
request_id	String	• Request ID. • The value must be in standard UUID format.
sub_network_interfaces	Array of **SubNetworkInterface** objects	• Supplementary network interfaces.
page_info	**PageInfo** object	Pagination information.

Table 5-135 SubNetworkInterface

Parameter	Type	Description
id	String	• Unique identifier of the supplementary network interface. • The value is in UUID format with hyphens (-).
virsubnet_id	String	• Virtual subnet ID, also the subnet ID, which is the same as the network ID displayed on the subnet summary page on the console. • The value must be in standard UUID format.
private_ip_address	String	• Private IPv4 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
ipv6_ip_address	String	• Private IPv6 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
mac_address	String	• MAC address of the supplementary network interface. • The value is a valid MAC address assigned by the system randomly.

Parameter	Type	Description
parent_device_id	String	• Device ID. • The value must be in standard UUID format.
parent_id	String	• ID of the elastic network interface. • The value must be in standard UUID format.
description	String	• Description of the supplementary network interface. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	• VPC ID of the supplementary network interface. • The value must be in standard UUID format.
vlan_id	Integer	• VLAN ID of the supplementary network interface. • The value can be from 1 to 4094. • Each supplementary network interface of an elastic network interface has a unique VLAN ID.
security_enabled	Boolean	• Whether the security option is enabled for the supplementary network interface. If the option is not enabled, the security group does not take effect.
security_groups	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"] • The default value is the default security group.
tags	Array of strings	• Tags of the supplementary network interface.
project_id	String	• Project ID of the supplementary network interface.
created_at	String	• The time when the supplementary network interface is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Table 5-136 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page
current_count	Integer	Total number of records on the current page
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Example Request

List all supplementary network interfaces.

```
GET https://{Endpoint}/v3/{project_id}/vpc/sub-network-interfaces?
vpc_id=63b97e6b-3598-430f-9eb8-1caf06937be8
```

Example Response

When the status code is **200**, the response parameters are as follows:

OK

```
{
  "request_id" : "e4cb9e3a-7b99-41c9-afd8-1630fe313299",
  "sub_network_interfaces" : [ {
    "id" : "2be868f2-f7c9-48db-abc0-eea0b9105b0d",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
    "private_ip_address" : "10.0.0.225",
    "ipv6_ip_address" : null,
    "mac_address" : "fa:16:3e:48:f8:6f",
    "parent_device_id" : "1ab01f1d-4ef7-4d83-82be-802b3aca0223",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : "63b97e6b-3598-430f-9eb8-1caf06937be8",
    "description" : null,
    "parent_id" : "637748df-2986-4350-8303-95d259580fb3",
    "vlan_id" : 2787,
    "tags" : [ ],
    "created_at" : "2020-05-19T01:16:25Z"
  }, {
    "id" : "55761e2d-8f72-42c0-9874-98e9885bf0fe",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
    "private_ip_address" : "10.0.3.55",
    "ipv6_ip_address" : null,
    "mac_address" : "fa:16:3e:c2:2c:ba",
    "parent_device_id" : "1ab01f1d-4ef7-4d83-82be-802b3aca0223",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : "63b97e6b-3598-430f-9eb8-1caf06937be8",
    "description" : null,
    "parent_id" : "637748df-2986-4350-8303-95d259580fb3",
    "vlan_id" : 799,
    "tags" : [ ],
    "created_at" : "2020-05-19T01:16:31Z"
  } ],
  "page_info" : {
    "next_marker" : "55761e2d-8f72-42c0-9874-98e9885bf0fe",
    "previous_marker" : "2be868f2-f7c9-48db-abc0-eea0b9105b0d",
    "current_count" : 2
```



```
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.5.4 Querying Details of a Supplementary Network Interface

Function

This API is used to query details about a supplementary network interface.

URI

GET /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}

Table 5-137 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
sub_network_interface_id	Yes	String	Unique identifier of the supplementary network interface.

Request Parameters

None

Response Parameters

When the status code is **200**, the response parameters are as follows:

Table 5-138 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.

Parameter	Type	Description
sub_network_interface	**SubNetworkInterface** object	Response body of a supplementary network interface.

Table 5-139 SubNetworkInterface

Parameter	Type	Description
id	String	• Unique identifier of the supplementary network interface. • The value is in UUID format with hyphens (-).
virsubnet_id	String	• Virtual subnet ID, also the subnet ID, which is the same as the network ID displayed on the subnet summary page on the console. • The value must be in standard UUID format.
private_ip_address	String	• Private IPv4 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
ipv6_ip_address	String	• Private IPv6 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
mac_address	String	• MAC address of the supplementary network interface. • The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	• Device ID. • The value must be in standard UUID format.
parent_id	String	• ID of the elastic network interface. • The value must be in standard UUID format.
description	String	• Description of the supplementary network interface. • The value can contain up to 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
vpc_id	String	• VPC ID of the supplementary network interface. • The value must be in standard UUID format.
vlan_id	Integer	• VLAN ID of the supplementary network interface. • The value can be from 1 to 4094. • Each supplementary network interface of an elastic network interface has a unique VLAN ID.
security_enabled	Boolean	• Whether the security option is enabled for the supplementary network interface. If the option is not enabled, the security group does not take effect.
security_groups	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"] • The default value is the default security group.
tags	Array of strings	• Tags of the supplementary network interface.
project_id	String	• Project ID of the supplementary network interface.
created_at	String	• The time when the supplementary network interface is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Request

Query details about a supplementary network interface.

```
GET https://{Endpoint}/v3/{project_id}/vpc/sub-network-interfaces/2be868f2-f7c9-48db-abc0-eea0b9105b0d
```

Example Response

When the status code is **200**, the response parameters are as follows:

OK

```
{
  "sub_network_interface" : {
    "id" : "2be868f2-f7c9-48db-abc0-eea0b9105b0d",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
    "private_ip_address" : "10.0.0.225",
    "ipv6_ip_address" : null,
    "mac_address" : "fa:16:3e:48:f8:6f",
```



```
    "parent_device_id" : "1ab01f1d-4ef7-4d83-82be-802b3aca0223",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : "63b97e6b-3598-430f-9eb8-1caf06937be8",
    "description" : null,
    "parent_id" : "637748df-2986-4350-8303-95d259580fb3",
    "vlan_id" : 2787,
    "tags" : [ ],
    "created_at" : "2020-05-19T01:16:25Z"
  },
  "request_id" : "ceb6273e-1ec9-4168-ac11-3dfeaacfc889"
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.5.5 Querying the Number of Supplementary Network Interfaces

Function

This API is used to query the number of supplementary network interfaces.

URI

GET /v3/{project_id}/vpc/sub-network-interfaces/count

Table 5-140 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

None

Response Parameters

When the status code is **200**, the response parameters are as follows:

Table 5-141 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
sub_network_interfaces	Integer	Number of supplementary network interfaces.

Example Request

Query the number of supplementary network interfaces.

```
GET https://{Endpoint}/v3/{project_id}/vpc/sub-network-interfaces/count
```

Example Response

When the status code is **200**, the response parameters are as follows:

OK

```
{
  "sub_network_interfaces" : 2,
  "request_id" : "4a79f1f7-67eb-43be-a8be-eb57ba894f90"
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.5.6 Updating a Supplementary Network Interface

Function

This API is used to update a supplementary network interface.

URI

PUT /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}

Table 5-142 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
sub_network_interface_id	Yes	String	Unique identifier of the supplementary network interface.

Request Parameters

Table 5-143 Request body parameter

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	• Whether to only send the check request. • The value can be: – **true**: A check request will be sent and no supplementary network interface will be updated. Check items include mandatory parameters, request format, and permission verification. If the check fails, the system returns an error. If the check succeeds, response code 202 will be returned. – **false** (default value): A request will be sent and a supplementary network interface will be updated.
sub_network_interface	Yes	**UpdateSubNetworkInterfaceOption** object	Request body for updating a supplementary network interface.

Table 5-144 UpdateSubNetworkInterfaceOption

Parameter	Mandatory	Type	Description
description	No	String	• Description of the supplementary network interface. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
security_groups	No	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]

Response Parameters

When the status code is **200**, the response parameters are as follows:

Table 5-145 Response body parameters

Parameter	Type	Description
request_id	String	Request ID.
sub_network_interface	**SubNetworkInterface** object	Response body for updating a supplementary network interface.

Table 5-146 SubNetworkInterface

Parameter	Type	Description
id	String	• Unique identifier of the supplementary network interface. • The value is in UUID format with hyphens (-).
virsubnet_id	String	• Virtual subnet ID, also the subnet ID, which is the same as the network ID displayed on the subnet summary page on the console. • The value must be in standard UUID format.
private_ip_address	String	• Private IPv4 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.

Parameter	Type	Description
ipv6_ip_address	String	• Private IPv6 address of the supplementary network interface. • The value must be within the virtual subnet. If this parameter is left blank, an IP address will be randomly assigned.
mac_address	String	• MAC address of the supplementary network interface. • The value is a valid MAC address assigned by the system randomly.
parent_device_id	String	• Device ID. • The value must be in standard UUID format.
parent_id	String	• ID of the elastic network interface. • The value must be in standard UUID format.
description	String	• Description of the supplementary network interface. • The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
vpc_id	String	• VPC ID of the supplementary network interface. • The value must be in standard UUID format.
vlan_id	Integer	• VLAN ID of the supplementary network interface. • The value can be from 1 to 4094. • Each supplementary network interface of an elastic network interface has a unique VLAN ID.
security_enabled	Boolean	• Whether the security option is enabled for the supplementary network interface. If the option is not enabled, the security group does not take effect.
security_groups	Array of strings	• Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"] • The default value is the default security group.
tags	Array of strings	• Tags of the supplementary network interface.
project_id	String	• Project ID of the supplementary network interface.

Parameter	Type	Description
created_at	String	• The time when the supplementary network interface is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Request

Change the security group that is associated with the supplementary network interface whose ID is 2be868f2-f7c9-48db-abc0-eea0b9105b0d.

```
PUT https://{Endpoint}/v3/8c6fb137a48a428aaf9a0229dca4edb3/vpc/sub-network-interfaces/2be868f2-f7c9-48db-abc0-eea0b9105b0d

{
  "sub_network_interface" : {
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ]
  }
}
```

Example Response

When the status code is **200**, the response parameters are as follows:

OK

```
{
  "sub_network_interface" : {
    "id" : "2be868f2-f7c9-48db-abc0-eea0b9105b0d",
    "project_id" : "8c6fb137a48a428aaf9a0229dca4edb3",
    "virsubnet_id" : "08278e6c-61ca-46c1-9fc3-0d4f6c12f193",
    "private_ip_address" : "10.0.0.225",
    "ipv6_ip_address" : null,
    "mac_address" : "fa:16:3e:48:f8:6f",
    "parent_device_id" : "1ab01f1d-4ef7-4d83-82be-802b3aca0223",
    "security_groups" : [ "6727c950-9f01-47a2-a7aa-7d3686c4c95b" ],
    "vpc_id" : "63b97e6b-3598-430f-9eb8-1caf06937be8",
    "description" : null,
    "parent_id" : "637748df-2986-4350-8303-95d259580fb3",
    "vlan_id" : 2787,
    "tags" : [ ],
    "created_at" : "2020-05-19T01:16:25Z"
  },
  "request_id" : "ceb6273e-1ec9-4168-ac11-3dfeaacfc889"
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.5.7 Deleting a Supplementary Network Interface

Function

This API is used to delete a supplementary network interface.

URI

DELETE /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}

Table 5-147 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
sub_network_interface_id	Yes	String	Unique identifier of the supplementary network interface.

Request Parameters

None

Response Parameters

None

Example Request

Delete a supplementary network interface.

```
DELETE https://{Endpoint}/v3/{project_id}/vpc/sub-network-interfaces/2be868f2-f7c9-48db-abc0-eea0b9105b0d
```

Example Response

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See **Error Codes**.

5.6 Traffic Mirror Sessions

5.6.1 Querying Traffic Mirror Sessions

Function

This API is used to query traffic mirror sessions.

URI

GET /v3/{project_id}/vpc/traffic-mirror-sessions

Table 5-148 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 5-149 Query Parameters

Parameter	Mandatory	Type	Description
created_at	No	String	Sort by creation time.
description	No	String	Filter by mirror session description.
enabled	No	String	Filter by enabled.
id	No	String	Filter or sort by mirror session ID.
name	No	String	Filter or sort by mirror session name.
packet_length	No	String	Filter by maximum transmission unit (MTU).
priority	No	String	Filter by mirror session priority.
traffic_mirror_filter_id	No	String	Filter by filter ID.
traffic_mirror_target_id	No	String	Filter by mirror target ID.
traffic_mirror_target_type	No	String	Filter by mirror target type.
type	No	String	Filter by mirror source type.

Parameter	Mandatory	Type	Description
updated_at	No	String	Sort by update time.
virtual_network_id	No	String	Filter by VNI.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-150 Response body parameters

Parameter	Type	Description
traffic_mirror_sessions	Array of **TrafficMirrorSession** objects	Traffic mirror sessions.
page_info	**PageInfo** object	Pagination information.
request_id	String	Request ID.

Table 5-151 TrafficMirrorSession

Parameter	Type	Description
id	String	Traffic mirror session ID.
project_id	String	Project ID.
name	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.

Parameter	Type	Description
traffic_mirror_sources	Array of strings	Mirror source IDs. An elastic network interface can be used as a mirror source. Each mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Mirror target ID.
traffic_mirror_target_type	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).
virtual_network_id	Integer	VNI, which is used to distinguish mirrored traffic of different sessions. Value range: 0-16777215. Default value: 1
packet_length	Integer	Maximum transmission unit (MTU). Value range: 1-1460 Default value: 96
priority	Integer	Mirror session priority. Value range: 1-32766
enabled	Boolean	Whether to enable a mirror session. The value can be true or false. Default value: false
type	String	Supported mirror source type. The value can be eni (elastic network interface).
created_at	String	Time when a traffic mirror session is created.
updated_at	String	Time when a traffic mirror session is updated.

Table 5-152 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page.
current_count	Integer	Total number of records on the current page.
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Example Requests

Querying traffic mirror sessions.

```
GET http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-sessions
```

Example Responses

Status code: 200

OK


```
{
  "request_id" : "f87354b7-eecd-4b64-87f6-bfd6430e33bd",
  "traffic_mirror_sessions" : [ {
    "name" : "test-session",
    "created_at" : "2023-03-14T08:44:12.000+00:00",
    "updated_at" : "2023-03-14T08:44:12.000+00:00",
    "id" : "6cc12480-5a92-4aed-99fb-07c52cc98961",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982a" ],
    "traffic_mirror_target_id" : "029ab12b-dc38-4228-b146-44975bf55250",
    "traffic_mirror_target_type" : "eni",
    "virtual_network_id" : 1,
    "packet_length" : 96,
    "priority" : 9,
    "enabled" : true,
    "type" : "eni"
  } ],
  "page_info" : {
    "previous_marker" : "6cc12480-5a92-4aed-99fb-07c52cc98961",
    "current_count" : 1
  }
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.6.2 Querying Details About a Traffic Mirror Session

Function

This API is used to query details about a traffic mirror session.

URI

GET /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}

Table 5-153 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_session_id	Yes	String	Traffic mirror session ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-154 Response body parameters

Parameter	Type	Description
traffic_mirror_session	**TrafficMirrorSession** object	Traffic mirror session.
request_id	String	Request ID.

Table 5-155 TrafficMirrorSession

Parameter	Type	Description
id	String	Traffic mirror session ID.
project_id	String	Project ID.
name	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.

Parameter	Type	Description
traffic_mirror_sources	Array of strings	Mirror source IDs. An elastic network interface can be used as a mirror source. Each mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Mirror target ID.
traffic_mirror_target_type	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).
virtual_network_id	Integer	VNI, which is used to distinguish mirrored traffic of different sessions. Value range: 0-16777215. Default value: 1
packet_length	Integer	Maximum transmission unit (MTU). Value range: 1-1460 Default value: 96
priority	Integer	Mirror session priority. Value range: 1-32766
enabled	Boolean	Whether to enable a mirror session. The value can be true or false. Default value: false
type	String	Supported mirror source type. The value can be eni (elastic network interface).
created_at	String	Time when a traffic mirror session is created.
updated_at	String	Time when a traffic mirror session is updated.

Example Requests

Querying details about a traffic mirror session.

```
GET http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-sessions/e15a6e40-2580-4949-bf2a-55ee7cd49392
```

Example Responses

Status code: 200

OK

```
{
  "traffic_mirror_session" : {
```



```
    "name" : "test-session",
    "created_at" : "2023-02-23T06:57:39.000+00:00",
    "updated_at" : "2023-02-23T06:57:39.000+00:00",
    "id" : "e15a6e40-2580-4949-bf2a-55ee7cd49392",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982a" ],
    "traffic_mirror_target_id" : "1adbc9b3-df85-4343-948a-d129536fa309",
    "traffic_mirror_target_type" : "eni",
    "virtual_network_id" : 1,
    "packet_length" : 96,
    "priority" : 6,
    "enabled" : true,
    "type" : "eni"
  },
  "request_id" : "be17b2e9-098c-4b56-ac0c-97e6b6413f12"
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.6.3 Creating a Traffic Mirror Session

Function

This API is used to create a traffic mirror session.

URI

POST /v3/{project_id}/vpc/traffic-mirror-sessions

Table 5-156 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 5-157 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_session	Yes	**CreateTrafficMirrorSessionOption** object	Traffic mirror session.

Table 5-158 CreateTrafficMirrorSessionOption

Parameter	Mandatory	Type	Description
name	Yes	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	Yes	String	Traffic mirror filter ID.
traffic_mirror_sources	Yes	Array of strings	Mirror source IDs. An elastic network interface can be used as a mirror source. Each mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	Yes	String	Mirror target ID.
traffic_mirror_target_type	Yes	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).

Parameter	Mandatory	Type	Description
virtual_network_id	No	String	VNI, which is used to distinguish mirrored traffic of different sessions. Value range: 0-16777215 Default value: 1
packet_length	No	String	Maximum transmission unit (MTU). Value range: 1-1460 Default value: 96
priority	Yes	Integer	Mirror session priority. Value range: 1-32766
enabled	No	String	Whether to enable a mirror session. The value can be true or false. Default value: false
type	No	String	Supported mirror source type. The value can be eni (elastic network interface).

Response Parameters

Status code: 201

Table 5-159 Response body parameters

Parameter	Type	Description
traffic_mirror_session	**TrafficMirrorSession** object	Traffic mirror session.
request_id	String	Request ID.

Table 5-160 TrafficMirrorSession

Parameter	Type	Description
id	String	Traffic mirror session ID.
project_id	String	Project ID.

Parameter	Type	Description
name	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
traffic_mirror_sources	Array of strings	Mirror source IDs. An elastic network interface can be used as a mirror source. Each mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Mirror target ID.
traffic_mirror_target_type	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).
virtual_network_id	Integer	VNI, which is used to distinguish mirrored traffic of different sessions. Value range: 0-16777215. Default value: 1
packet_length	Integer	Maximum transmission unit (MTU). Value range: 1-1460 Default value: 96
priority	Integer	Mirror session priority. Value range: 1-32766
enabled	Boolean	Whether to enable a mirror session. The value can be true or false. Default value: false
type	String	Supported mirror source type. The value can be eni (elastic network interface).
created_at	String	Time when a traffic mirror session is created.
updated_at	String	Time when a traffic mirror session is updated.

Example Requests

Create a traffic mirror session named test-session.

```
POST http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-sessions

{
  "traffic_mirror_session" : {
    "name" : "test-session",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982a" ],
    "traffic_mirror_target_id" : "c9f8acef-d550-4fbe-be7c-e8bfd3501dc1",
    "traffic_mirror_target_type" : "eni",
    "priority" : 11
  }
}
```

Example Responses

Status code: 201

Created

```
{
  "traffic_mirror_session" : {
    "name" : "test-session",
    "created_at" : "2023-03-23T10:53:12.000+00:00",
    "updated_at" : "2023-03-23T10:53:12.000+00:00",
    "id" : "16538eda-7e94-4b90-b5f3-a653f62dc817",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982a" ],
    "traffic_mirror_target_id" : "c9f8acef-d550-4fbe-be7c-e8bfd3501dc1",
    "traffic_mirror_target_type" : "eni",
    "virtual_network_id" : 1,
    "packet_length" : 96,
    "priority" : 11,
    "enabled" : true,
    "type" : "eni"
  },
  "request_id" : "9a880225-1d2f-461e-8d8e-1866bfda77db"
}
```

Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

5.6.4 Updating a Traffic Mirror Session

Function

This API is used to update a traffic mirror session.

URI

PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}

Table 5-161 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_session_id	Yes	String	Traffic mirror session ID.

Request Parameters

Table 5-162 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_session	Yes	**UpdateTrafficMirrorSessionOption** object	Traffic mirror session.

Table 5-163 UpdateTrafficMirrorSessionOption

Parameter	Mandatory	Type	Description
name	No	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	No	String	Traffic mirror filter ID.
traffic_mirror_target_id	No	String	Mirror target ID.

Parameter	Mandatory	Type	Description
traffic_mirror_target_type	No	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).
virtual_network_id	No	Integer	VNI, which is used to distinguish mirrored traffic of different sessions for a mirror target. Value range: 0-16777215
packet_length	No	Integer	Maximum transmission unit (MTU). Value range: 1-1460
priority	No	Integer	Mirror session priority. Value range: 1-32766
enabled	No	String	Whether to enable a mirror session. The value can be true or false.

Response Parameters

Status code: 200

Table 5-164 Response body parameters

Parameter	Type	Description
traffic_mirror_session	**TrafficMirrorSession** object	Traffic mirror session.
request_id	String	Request ID.

Table 5-165 TrafficMirrorSession

Parameter	Type	Description
id	String	Traffic mirror session ID.
project_id	String	Project ID.

Parameter	Type	Description
name	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
traffic_mirror_sources	Array of strings	Mirror source IDs. An elastic network interface can be used as a mirror source. Each mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Mirror target ID.
traffic_mirror_target_type	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).
virtual_network_id	Integer	VNI, which is used to distinguish mirrored traffic of different sessions. Value range: 0-16777215. Default value: 1
packet_length	Integer	Maximum transmission unit (MTU). Value range: 1-1460 Default value: 96
priority	Integer	Mirror session priority. Value range: 1-32766
enabled	Boolean	Whether to enable a mirror session. The value can be true or false. Default value: false
type	String	Supported mirror source type. The value can be eni (elastic network interface).
created_at	String	Time when a traffic mirror session is created.
updated_at	String	Time when a traffic mirror session is updated.

Example Requests

Update the traffic mirror session with ID of 16538eda-7e94-4b90-b5f3-a653f62dc817, mirror target type of elb, and mirror target ID of c9f8acef-d550-4fbe-be7c-e8bfd3501dc1.

```
PUT http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-sessions/16538eda-7e94-4b90-b5f3-a653f62dc817

{
  "traffic_mirror_session" : {
    "traffic_mirror_target_id" : "c9f8acef-d550-4fbe-be7c-e8bfd3501dc1",
    "traffic_mirror_target_type" : "elb"
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "traffic_mirror_session" : {
    "name" : "test-session",
    "created_at" : "2023-03-23T10:53:12.000+00:00",
    "updated_at" : "2023-03-23T10:56:54.000+00:00",
    "id" : "16538eda-7e94-4b90-b5f3-a653f62dc817",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982a" ],
    "traffic_mirror_target_id" : "c9f8acef-d550-4fbe-be7c-e8bfd3501dc1",
    "traffic_mirror_target_type" : "elb",
    "virtual_network_id" : 1,
    "packet_length" : 96,
    "priority" : 11,
    "enabled" : true,
    "type" : "eni"
  },
  "request_id" : "a7ee4a0e-12e9-457a-b739-46bffb2e7bbb"
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.6.5 Deleting a Traffic Mirror Session

Function

This API is used to delete a traffic mirror session.

URI

DELETE /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}

Table 5-166 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_session_id	Yes	String	Traffic mirror session ID.

Request Parameters

None

Response Parameters

None

Example Requests

Deleting a traffic mirror session.

```
DELETE http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-sessions/16538eda-7e94-4b90-b5f3-a653f62dc817
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See **Error Codes**.

5.6.6 Disassociating a Traffic Mirror Source from a Traffic Mirror Session

Function

This API is used to disassociate a traffic mirror source from a traffic mirror session.

URI

PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/remove-sources

Table 5-167 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_session_id	Yes	String	Traffic mirror session ID.

Request Parameters

Table 5-168 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_session	Yes	**TrafficMirrorSourcesOption** object	Traffic mirror session.

Table 5-169 TrafficMirrorSourcesOption

Parameter	Mandatory	Type	Description
traffic_mirror_sources	Yes	Array of strings	Traffic mirror source IDs.

Response Parameters

Status code: 200

Table 5-170 Response body parameters

Parameter	Type	Description
traffic_mirror_session	**TrafficMirrorSession** object	Traffic mirror session.
request_id	String	Request ID.

Table 5-171 TrafficMirrorSession

Parameter	Type	Description
id	String	Traffic mirror session ID.
project_id	String	Project ID.
name	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
traffic_mirror_sources	Array of strings	Mirror source IDs. An elastic network interface can be used as a mirror source. Each mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Mirror target ID.
traffic_mirror_target_type	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).
virtual_network_id	Integer	VNI, which is used to distinguish mirrored traffic of different sessions. Value range: 0-16777215. Default value: 1
packet_length	Integer	Maximum transmission unit (MTU). Value range: 1-1460 Default value: 96
priority	Integer	Mirror session priority. Value range: 1-32766
enabled	Boolean	Whether to enable a mirror session. The value can be true or false. Default value: false
type	String	Supported mirror source type. The value can be eni (elastic network interface).

Parameter	Type	Description
created_at	String	Time when a traffic mirror session is created.
updated_at	String	Time when a traffic mirror session is updated.

Example Requests

Disassociate the mirror source with ID of 6134900d-31a6-4b71-8453-dbca7f26982a from the mirror session with ID of e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
PUT https://{endpoint}/v3/{project_id}/vpc/traffic-mirror-sessions/e15a6e40-2580-4949-bf2a-55ee7cd49392/remove-sources

{
  "traffic_mirror_session" : {
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982a" ]
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "traffic_mirror_session" : {
    "name" : "test-session",
    "created_at" : "2023-02-23T06:57:39.000+00:00",
    "updated_at" : "2023-02-23T06:57:39.000+00:00",
    "id" : "e15a6e40-2580-4949-bf2a-55ee7cd49392",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "traffic_mirror_sources" : [ ],
    "traffic_mirror_target_id" : "",
    "traffic_mirror_target_type" : "",
    "virtual_network_id" : 1,
    "packet_length" : 96,
    "priority" : 6,
    "enabled" : true,
    "type" : "eni"
  },
  "request_id" : "6f107fc1-93be-4d5a-af71-4099da7eeaa9"
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.6.7 Associating a Traffic Mirror Source with a Traffic Mirror Session

Function

This API is used to associate a traffic mirror source with a traffic mirror session.

URI

PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/add-sources

Table 5-172 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_session_id	Yes	String	Traffic mirror session ID.

Request Parameters

Table 5-173 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_session	Yes	**TrafficMirrorSourcesOption** object	Traffic mirror session.

Table 5-174 TrafficMirrorSourcesOption

Parameter	Mandatory	Type	Description
traffic_mirror_sources	Yes	Array of strings	Traffic mirror source IDs.

Response Parameters

Status code: 200

Table 5-175 Response body parameters

Parameter	Type	Description
traffic_mirror_session	**TrafficMirrorSession** object	Traffic mirror session.
request_id	String	Request ID.

Table 5-176 TrafficMirrorSession

Parameter	Type	Description
id	String	Traffic mirror session ID.
project_id	String	Project ID.
name	String	Traffic mirror session name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Description of a traffic mirror session. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
traffic_mirror_sources	Array of strings	Mirror source IDs. An elastic network interface can be used as a mirror source. Each mirror session can have up to 10 mirror sources by default.
traffic_mirror_target_id	String	Mirror target ID.
traffic_mirror_target_type	String	Mirror target type. The value can be eni (elastic network interface) or elb (private network load balancer).
virtual_network_id	Integer	VNI, which is used to distinguish mirrored traffic of different sessions. Value range: 0-16777215. Default value: 1
packet_length	Integer	Maximum transmission unit (MTU). Value range: 1-1460 Default value: 96

Parameter	Type	Description
priority	Integer	Mirror session priority. Value range: 1-32766
enabled	Boolean	Whether to enable a mirror session. The value can be true or false. Default value: false
type	String	Supported mirror source type. The value can be eni (elastic network interface).
created_at	String	Time when a traffic mirror session is created.
updated_at	String	Time when a traffic mirror session is updated.

Example Requests

Associate the mirror source 6134900d-31a6-4b71-8453-dbca7f26982e with the mirror session e15a6e40-2580-4949-bf2a-55ee7cd49392.

```
PUT https://{endpoint}/v3/{project_id}/vpc/traffic-mirror-sessions/e15a6e40-2580-4949-bf2a-55ee7cd49392/add-sources

{
  "traffic_mirror_session" : {
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982e" ]
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "traffic_mirror_session" : {
    "name" : "test-session",
    "created_at" : "2023-02-23T06:57:39.000+00:00",
    "updated_at" : "2023-02-23T06:57:39.000+00:00",
    "id" : "e15a6e40-2580-4949-bf2a-55ee7cd49392",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "traffic_mirror_sources" : [ "6134900d-31a6-4b71-8453-dbca7f26982a" ],
    "traffic_mirror_target_id" : "1adbc9b3-df85-4343-948a-d129536fa309",
    "traffic_mirror_target_type" : "eni",
    "virtual_network_id" : 1,
    "packet_length" : 96,
    "priority" : 6,
    "enabled" : true,
    "type" : "eni"
  },
  "request_id" : "be17b2e9-098c-4b56-ac0c-97e6b6413f12"
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.7 Traffic Mirror Filters

5.7.1 Creating a Traffic Mirror Filter

Function

This API is used to create a traffic mirror filter.

URI

POST /v3/{project_id}/vpc/traffic-mirror-filters

Table 5-177 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 5-178 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_filter	Yes	**CreateTrafficMirrorFilterOption** object	Traffic mirror filter.

Table 5-179 CreateTrafficMirrorFilterOption

Parameter	Mandatory	Type	Description
description	No	String	Description of a traffic mirror filter. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
name	Yes	String	Traffic mirror filter name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Response Parameters

Status code: 201

Table 5-180 Response body parameters

Parameter	Type	Description
traffic_mirror_filter	**TrafficMirrorFilter** object	Traffic mirror filter.
request_id	String	Request ID.

Table 5-181 TrafficMirrorFilter

Parameter	Type	Description
id	String	Traffic mirror filter ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
name	String	Traffic mirror filter name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
ingress_rules	Array of **TrafficMirrorFilterRule** objects	Inbound mirror filter rules.
egress_rules	Array of **TrafficMirrorFilterRule** objects	Outbound mirror filter rules.
created_at	String	Time when a traffic mirror filter is created.
updated_at	String	Time when a traffic mirror filter is updated.

Table 5-182 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.

Parameter	Type	Description
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Example Requests

Create a traffic mirror filter named test1 with description description.

```
POST https://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filters

{
  "traffic_mirror_filter" : {
    "name" : "test1",
    "description" : "description"
  }
}
```

Example Responses

Status code: 201

Created

```
{
  "traffic_mirror_filter" : {
    "id" : "59d2b2e7-0d35-41f7-a12e-f7699366cd21",
    "project_id" : "49a42f378df747bf8b8f6a70e25b63fb",
    "name" : "test1",
    "description" : "description",
    "ingress_rules" : [ ],
    "egress_rules" : [ ],
    "type" : "eni",
    "created_at" : "2022-08-29T06:22:01.000+00:00",
    "updated_at" : "2022-08-29T06:22:01.000+00:00"
  },
  "request_id" : "f05abcd9-fa75-43a5-a795-b3d8e8b7a9e9"
}
```


Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

5.7.2 Querying Traffic Mirror Filters

Function

This API is used to query traffic mirror filters.

URI

GET /v3/{project_id}/vpc/traffic-mirror-filters

Table 5-183 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 5-184 Query Parameters

Parameter	Mandatory	Type	Description
created_at	No	String	Sort by creation time.
description	No	String	Filter by description.
id	No	String	Query or sort by ID.
name	No	String	Filter or sort by name.
updated_at	No	String	Sort by update time.
type	No	String	Sort by type.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-185 Response body parameters

Parameter	Type	Description
traffic_mirror_filters	Array of **TrafficMirrorFilter** objects	Traffic mirror filters.
page_info	**PageInfo** object	Pagination information.
request_id	String	Request ID.

Table 5-186 TrafficMirrorFilter

Parameter	Type	Description
id	String	Traffic mirror filter ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
name	String	Traffic mirror filter name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
ingress_rules	Array of **TrafficMirrorFilterRule** objects	Inbound mirror filter rules.
egress_rules	Array of **TrafficMirrorFilterRule** objects	Outbound mirror filter rules.
created_at	String	Time when a traffic mirror filter is created.
updated_at	String	Time when a traffic mirror filter is updated.

Table 5-187 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.

Parameter	Type	Description
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Table 5-188 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page.
current_count	Integer	Total number of records on the current page.
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Example Requests

Querying traffic mirror filters.

```
GET http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filters
```

Example Responses

Status code: 200

OK

```
{
  "request_id" : "05e4a009-74aa-47cb-8055-c3da26a51737",
  "traffic_mirror_filters" : [ {
    "id" : "59d2b2e7-0d35-41f7-a12e-f7699366cd21",
    "project_id" : "49a42f378df747bf8b8f6a70e25b63fb",
    "name" : "test1",
    "description" : "new_filter",
    "ingress_rules" : [ ],
    "egress_rules" : [ ],
    "type" : "eni",
    "created_at" : "2022-08-29T06:22:01.000+00:00",
    "updated_at" : "2022-08-29T06:22:01.000+00:00"
  } ],
  "page_info" : {
    "previous_marker" : "180edd76-ab7e-4039-acc2-239ff89243e8",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.7.3 Querying Details About a Traffic Mirror Filter

Function

This API is used to query details about a traffic mirror filter.

URI

GET /v3/{project_id}/vpc/traffic-mirror-filters/{traffic_mirror_filter_id}

Table 5-189 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_filter_id	Yes	String	Traffic mirror filter ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-190 Response body parameters

Parameter	Type	Description
traffic_mirror_filter	TrafficMirrorFilter object	Traffic mirror filter.
request_id	String	Request ID.

Table 5-191 TrafficMirrorFilter

Parameter	Type	Description
id	String	Traffic mirror filter ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
name	String	Traffic mirror filter name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
ingress_rules	Array of **TrafficMirrorFilterRule** objects	Inbound mirror filter rules.
egress_rules	Array of **TrafficMirrorFilterRule** objects	Outbound mirror filter rules.
created_at	String	Time when a traffic mirror filter is created.
updated_at	String	Time when a traffic mirror filter is updated.

Table 5-192 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200

Parameter	Type	Description
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Example Requests

Querying details about a traffic mirror filter.

```
GET http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filters/59d2b2e7-0d35-41f7-a12e-f7699366cd21
```

Example Responses

Status code: 200

OK

```
{
  "traffic_mirror_filter" : {
    "id" : "59d2b2e7-0d35-41f7-a12e-f7699366cd21",
    "project_id" : "49a42f378df747bf8b8f6a70e25b63fb",
    "name" : "test1",
    "description" : "new_filter",
    "ingress_rules" : [ ],
    "egress_rules" : [ ],
    "type" : "eni",
    "created_at" : "2022-08-29T06:22:01.000+00:00",
    "updated_at" : "2022-08-29T06:22:01.000+00:00"
  },
  "request_id" : "f05abcd9-fa75-43a5-a795-b3d8e8b7a9e9"
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.7.4 Updating a Traffic Mirror Filter

Function

This API is used to update a traffic mirror filter.

URI

PUT /v3/{project_id}/vpc/traffic-mirror-filters/{traffic_mirror_filter_id}

Table 5-193 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_filter_id	Yes	String	Traffic mirror filter ID.

Request Parameters

Table 5-194 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_filter	Yes	**UpdateTrafficMirrorFilterOption** object	Traffic mirror filter.

Table 5-195 UpdateTrafficMirrorFilterOption

Parameter	Mandatory	Type	Description
description	No	String	Description of a traffic mirror filter. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
name	No	String	Traffic mirror filter name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Response Parameters

Status code: 200

Table 5-196 Response body parameters

Parameter	Type	Description
traffic_mirror_filter	**TrafficMirrorFilter** object	Traffic mirror filter.
request_id	String	Request ID.

Table 5-197 TrafficMirrorFilter

Parameter	Type	Description
id	String	Traffic mirror filter ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
name	String	Traffic mirror filter name. The value can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
ingress_rules	Array of **TrafficMirrorFilterRule** objects	Inbound mirror filter rules.
egress_rules	Array of **TrafficMirrorFilterRule** objects	Outbound mirror filter rules.
created_at	String	Time when a traffic mirror filter is created.
updated_at	String	Time when a traffic mirror filter is updated.

Table 5-198 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.

Parameter	Type	Description
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Example Requests

Change the name of the traffic mirror filter whose ID is 59d2b2e7-0d35-41f7-a12e-f7699366cd21 to test1.

```
PUT /v3/{project_id}/vpc/traffic-mirror-filters/59d2b2e7-0d35-41f7-a12e-f7699366cd21

{
  "traffic_mirror_filter" : {
    "name" : "test1",
    "description" : "description"
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "traffic_mirror_filter" : {
    "id" : "59d2b2e7-0d35-41f7-a12e-f7699366cd21",
    "project_id" : "49a42f378df747bf8b8f6a70e25b63fb",
    "name" : "test1",
    "description" : "description",
    "ingress_rules" : [ ],
    "egress_rules" : [ ],
    "type" : "eni",
    "created_at" : "2022-08-29T06:22:01.000+00:00",
    "updated_at" : "2022-08-29T06:22:01.000+00:00"
  },
  "request_id" : "f05abcd9-fa75-43a5-a795-b3d8e8b7a9e9"
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.7.5 Deleting a Traffic Mirror Filter

Function

This API is used to delete a traffic mirror filter.

URI

DELETE /v3/{project_id}/vpc/traffic-mirror-filters/{traffic_mirror_filter_id}

Table 5-199 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_filter_id	Yes	String	Traffic mirror filter ID.

Request Parameters

None

Response Parameters

None

Example Requests

Deleting a traffic mirror filter.

```
DELETE http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filters/59d2b2e7-0d35-41f7-a12e-f7699366cd21
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See **Error Codes**.

5.8 Traffic Mirror Filter Rules

5.8.1 Querying Traffic Mirror Filter Rules

Function

This API is used to query traffic mirror filter rules.

URI

GET /v3/{project_id}/vpc/traffic-mirror-filter-rules

Table 5-200 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 5-201 Query Parameters

Parameter	Mandatory	Type	Description
action	No	String	Filter by action.
description	No	String	Filter by description.
destination_cidr_block	No	String	Filter by destination CIDR block.
destination_port_range	No	String	Filter by destination port range.
direction	No	String	Filter by direction.
id	No	String	Filter or sort by ID.
priority	No	String	Filter by priority.

Parameter	Mandatory	Type	Description
protocol	No	String	Filter by protocol.
source_cidr_block	No	String	Filter by source CIDR block.
source_port_range	No	String	Filter by source port range.
traffic_mirror_filter_id	No	String	Filter by traffic mirror filter ID.
type	No	String	Filter by type.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-202 Response body parameters

Parameter	Type	Description
traffic_mirror_filter_rules	Array of **TrafficMirrorFilterRule** objects	Traffic mirror filter rules.
page_info	**PageInfo** object	Pagination information.
request_id	String	Request ID.

Table 5-203 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).

Parameter	Type	Description
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Table 5-204 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page.
current_count	Integer	Total number of records on the current page.

Parameter	Type	Description
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Example Requests

Querying traffic mirror filter rules.

```
GET http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filter-rules
```

Example Responses

Status code: 200

OK

```
{
  "request_id" : "38719a68-c7c1-4fe1-bf12-4bb049349174",
  "traffic_mirror_filter_rules" : [ {
    "created_at" : "2023-02-17T08:42:44.000+00:00",
    "updated_at" : "2023-02-17T08:42:44.000+00:00",
    "id" : "3daa97b5-ad58-477d-86a5-52b65257f94b",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "b765ba87-c0b4-4f1a-9ec3-d5b1d1ddb137",
    "direction" : "ingress",
    "protocol" : "ICMPV6",
    "ethertype" : "IPv4",
    "action" : "accept",
    "priority" : 16,
    "type" : "eni"
  } ],
  "page_info" : {
    "previous_marker" : "3daa97b5-ad58-477d-86a5-52b65257f94b",
    "current_count" : 1
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.8.2 Querying Details About a Traffic Mirror Filter Rule

Function

This API is used to query details about a traffic mirror filter rule.

URI

GET /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}

Table 5-205 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_filter_rule_id	Yes	String	Traffic mirror filter rule ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-206 Response body parameters

Parameter	Type	Description
traffic_mirror_filter_rule	**TrafficMirrorFilterRule** object	Traffic mirror filter rule.
request_id	String	Request ID.

Table 5-207 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.

Parameter	Type	Description
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Example Requests

Querying details about a traffic mirror filter rule.

```
GET http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filter-rules/2230d5a2-1868-4264-b917-0e06fa132898
```

Example Responses

Status code: 200

OK

```
{
  "traffic_mirror_filter_rule" : {
    "created_at" : "2023-02-23T16:08:45.000+00:00",
    "updated_at" : "2023-02-23T16:17:12.000+00:00",
    "id" : "2230d5a2-1868-4264-b917-0e06fa132898",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
```



```
    "description" : 123,
    "traffic_mirror_filter_id" : "417d7317-6c17-4428-a0f3-997d3e2293a0",
    "direction" : "ingress",
    "protocol" : "TCP",
    "ethertype" : "IPv4",
    "source_cidr_block" : "8.8.8.8/32",
    "destination_cidr_block" : "9.9.9.9/32",
    "destination_port_range" : "10-65535",
    "action" : "accept",
    "priority" : 20,
    "type" : "eni"
  },
  "request_id" : "ca9682cf-0680-469f-bb04-5b0f17b075d0"
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.8.3 Creating a Traffic Mirror Filter Rule

Function

This API is used to create a traffic mirror filter rule.

URI

POST /v3/{project_id}/vpc/traffic-mirror-filter-rules

Table 5-208 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Request Parameters

Table 5-209 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_filter_rule	Yes	**CreateTrafficMirrorFilterRuleOption** object	Traffic mirror filter rule.

Table 5-210 CreateTrafficMirrorFilterRuleOption

Parameter	Mandatory	Type	Description
description	No	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	Yes	String	Traffic mirror filter ID.
direction	Yes	String	Traffic direction. The value can be ingress or egress.
protocol	Yes	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
ethertype	Yes	String	IP address version of the mirrored traffic The value can be IPv4 or IPv6.
source_cidr_block	No	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	No	String	Destination CIDR block of the mirrored traffic.
source_port_range	No	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	No	String	Destination port range. Value range: 1-65535 Format: 80-200
action	Yes	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Yes	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.

Response Parameters

Status code: 201

Table 5-211 Response body parameters

Parameter	Type	Description
traffic_mirror_filter_rule	**TrafficMirrorFilterRule** object	Traffic mirror filter rule.
request_id	String	Request ID.

Table 5-212 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.

Parameter	Type	Description
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Example Requests

Add a traffic mirror filter rule in the inbound direction to the traffic mirror filter with ID of 417d7317-6c17-4428-a0f3-997d3e2293a0 and with source CIDR of 192.168.0.0/24.

```
POST http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filter-rules

{
  "traffic_mirror_filter_rule" : {
    "traffic_mirror_filter_id" : "417d7317-6c17-4428-a0f3-997d3e2293a0",
    "ethertype" : "ipv4",
    "direction" : "ingress",
    "protocol" : "ICMP",
    "source_cidr_block" : "192.168.0.0/24",
    "action" : "accept",
    "priority" : 29
  }
}
```

Example Responses

Status code: 201

Created

```
{
  "request_id" : "8dec5453-1690-4378-a976-40ba5e6d62ff",
  "traffic_mirror_filter_rule" : {
    "created_at" : "2023-03-22T07:07:55.000+00:00",
    "updated_at" : "2023-03-22T07:07:55.000+00:00",
    "id" : "1be5f64b-49a1-427d-a49e-9619cfb0492c",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "417d7317-6c17-4428-a0f3-997d3e2293a0",
    "direction" : "ingress",
    "protocol" : "ICMP",
    "ethertype" : "IPv4",
    "source_cidr_block" : "192.168.0.0/24",
    "action" : "accept",
    "priority" : 29,
```



```
  "type" : "eni"
 }
}
```

Status Codes

Status Code	Description
201	Created

Error Codes

See **Error Codes**.

5.8.4 Updating a Traffic Mirror Filter Rule

Function

This API is used to update a traffic mirror filter rule.

URI

PUT /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}

Table 5-213 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_filter_rule_id	Yes	String	Traffic mirror filter rule ID.

Request Parameters

Table 5-214 Request body parameters

Parameter	Mandatory	Type	Description
traffic_mirror_filter_rule	Yes	**UpdateTrafficMirrorFilterRuleOption** object	Traffic mirror filter rule.

Table 5-215 UpdateTrafficMirrorFilterRuleOption

Parameter	Mandatory	Type	Description
description	No	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
protocol	No	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
ethertype	No	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.
source_cidr_block	No	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	No	String	Destination CIDR block of the mirrored traffic.
source_port_range	No	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	No	String	Source port range. Value range: 1-65535 Format: 80-200
priority	No	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
action	No	String	Whether to accept or reject traffic. The value can be accept or reject.

Response Parameters

Status code: 200

Table 5-216 Response body parameters

Parameter	Type	Description
traffic_mirror_filter_rule	**TrafficMirrorFilterRule** object	Traffic mirror filter rule.
request_id	String	Request ID.

Table 5-217 TrafficMirrorFilterRule

Parameter	Type	Description
id	String	Traffic mirror filter rule ID.
project_id	String	Project ID.
description	String	Description of a traffic mirror filter rule. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
traffic_mirror_filter_id	String	Traffic mirror filter ID.
direction	String	Traffic direction. The value can be ingress or egress.
source_cidr_block	String	Source CIDR block of the mirrored traffic.
destination_cidr_block	String	Destination CIDR block of the mirrored traffic.
source_port_range	String	Source port range. Value range: 1-65535 Format: 80-200
destination_port_range	String	Destination port range. Value range: 1-65535 Format: 80-200
ethertype	String	IP address version of the mirrored traffic. The value can be IPv4 or IPv6.
protocol	String	Protocol of the mirrored traffic. The value can be TCP, UDP, ICMP, ICMPV6, or ALL.
action	String	Whether to accept or reject traffic. The value can be accept or reject.

Parameter	Type	Description
priority	Integer	Mirror filter rule priority. Value range: 1-65535. A smaller value indicates a higher priority.
created_at	String	Time when a traffic mirror filter rule is created.
updated_at	String	Time when a traffic mirror filter rule is updated.

Example Requests

Change action of the traffic mirror filter rule whose ID is 7c12805a-1b8d-40b5-ab23-a8fac480f2ec to reject.

```
PUT http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filter-rules/7c12805a-1b8d-40b5-ab23-a8fac480f2ec

{
  "traffic_mirror_filter_rule" : {
    "source_port_range" : "80-90",
    "destination_cidr_block" : "192.168.1.0/24",
    "source_cidr_block" : "10.0.0.0/8",
    "action" : "reject"
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "request_id" : "197e0ed1-f59f-473b-9363-74666a7d3710",
  "traffic_mirror_filter_rule" : {
    "created_at" : "2023-03-09T13:14:47.000+00:00",
    "updated_at" : "2023-03-09T13:16:43.000+00:00",
    "id" : "7c12805a-1b8d-40b5-ab23-a8fac480f2ec",
    "project_id" : "7365fcd452924e398ec4cc1fe39c0d12",
    "description" : "",
    "traffic_mirror_filter_id" : "417d7317-6c17-4428-a0f3-997d3e2293a0",
    "direction" : "ingress",
    "protocol" : "ICMP",
    "ethertype" : "IPv4",
    "source_cidr_block" : "80-90",
    "destination_cidr_block" : "192.168.1.0/24",
    "source_port_range" : "10.0.0.0/8",
    "action" : "reject",
    "priority" : 23,
    "type" : "eni"
  }
}
```


Status Codes

Status Code	Description
200	OK

Error Codes

See **Error Codes**.

5.8.5 Deleting a Traffic Mirror Filter Rule

Function

This API is used to delete a traffic mirror filter rule.

URI

DELETE /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}

Table 5-218 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.
traffic_mirror_filter_rule_id	Yes	String	Traffic mirror filter rule ID.

Request Parameters

None

Response Parameters

None

Example Requests

Deleting a traffic mirror filter rule.

```
DELETE http://{endpoint}/v3/{project_id}/vpc/traffic-mirror-filter-rules/2230d5a2-1868-4264-b917-0e06fa132898
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See **Error Codes**.

5.9 Network ACLs

5.9.1 Creating a Network ACL

Function

This API is used to create a network ACL.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

POST /v3/{project_id}/vpc/firewalls

Table 5-219 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 5-220 Request body parameter

Parameter	Mandatory	Type	Description
firewall	Yes	**CreateFirewallOption** object	Request body for creating a network ACL.

Parameter	Mandatory	Type	Description
dry_run	No	Boolean	Whether to only send the check request. The value can be: • **true**: A check request will be sent and no network ACL will be created. Check items include mandatory parameters, request format, and permission verification. If the check fails, the system returns an error. If the check succeeds, response code 202 will be returned. • **false**: A request will be sent and a network ACL will be created.

Table 5-221 CreateFirewallOption

Parameter	Mandatory	Type	Description
name	Yes	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	Provides supplementary information about the IP address group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
enterprise_project_id	No	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.

Parameter	Mandatory	Type	Description
tags	No	Array of ResourceTag objects	Network ACL tags.
admin_state_up	No	Boolean	Whether a network ACL is enabled. The default value is **true**. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.

Table 5-222 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	Yes	String	Tag value. Maximum length: **255**

Response Parameters

Status code: 201

Table 5-223 Response body parameters

Parameter	Type	Description
firewall	FirewallDetail object	Response body for creating a network ACL.
request_id	String	Request ID.

Table 5-224 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the IP address group. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmss. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmss. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.

Parameter	Type	Description
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-225 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-226 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-227 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Type	Description
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

Create a network ACL named **network_acl_test1**.

```
POST https://{Endpoint}/v3/{project_id}/vpc/firewalls

{
    "firewall": {
        "name": "network_acl_test1",
        "description": "network_acl_test1",
        "enterprise_project_id": "158ad39a-dab7-45a3-9b5a-2836b3cf93f9"
    }
}
```

Example Response

Status code: 201

Normal response for the POST operation of the API for creating a network ACL

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46",
    "updated_at" : "2022-04-07T07:30:46",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "ACTIVE",
    "tags" : [ ],
    "ingress_rules" : [ ],
    "egress_rules" : [ ],
    "associations" : [ ]
  }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.2 Querying Network ACLs

Function

This API is used to query network ACLs.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

GET /v3/{project_id}/vpc/firewalls

Table 5-228 Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID.

Table 5-229 Query parameters

Parameter	Mandatory	Type	Description
admin_state_up	No	Boolean	Whether a network ACL is enabled.
enterprise_project_id	No	Array	Enterprise project ID. This parameter can be used to filter the network ACLs of an enterprise project. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project. To obtain network ACLs of all enterprise projects, set this parameter to **all_granted_eps**.
id	No	Array	Unique ID of a network ACL, which can be used to filter the network ACL. Multiple IDs can be specified for filtering.

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records returned on each page. Value range: 0 to 2000
marker	No	String	Start resource ID of pagination query. If the parameter is left blank, only resources on the first page are queried.
name	No	Array	Name of a network ACL, which can be used to filter the network ACL. Multiple IDs can be specified for filtering.
status	No	String	Network ACL status. Enumerated values: • **ACTIVE** • **INACTIVE**

Request Parameters

None

Response Parameters

Status code: 200

Table 5-230 Response body parameters

Parameter	Type	Description
firewalls	Array of **ListFirewallDetail** objects	Network ACLs
page_info	**PageInfo** object	Pagination information
request_id	String	Request ID

Table 5-231 ListFirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.

Parameter	Type	Description
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about an IP address group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL

Table 5-232 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-233 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-234 PageInfo

Parameter	Type	Description
previous_marker	String	First record on the current page
current_count	Integer	Total number of records on the current page
next_marker	String	Last record on the current page. This parameter does not exist if the page is the last one.

Example Request

Query network ACLs.

```
GET https://{Endpoint}/v3/{project_id}/vpc/firewalls
```

Example Response

Status code: 200

OK

```
{
  "firewalls" : [ {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
    "updated_at" : "2022-04-07T07:30:46Z",
```



```
  "admin_state_up" : true,
  "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
  "status" : "ACTIVE",
  "tags" : [ ],
  "associations" : [ {
    "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
  } ]
 } ]
}
```

Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.3 Querying Details About a Network ACL

Function

This API is used to query details about a network ACL.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

GET /v3/{project_id}/vpc/firewalls/{firewall_id}

Table 5-235 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	ID of a network ACL, which uniquely identifies a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

None

Response Parameters

Status code: 200

Table 5-236 Response body parameters

Parameter	Type	Description
firewall	FirewallDetail object	Response body for querying a network ACL.
request_id	String	Request ID.

Table 5-237 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about an IP address group. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated. UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.

Parameter	Type	Description
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-238 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-239 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-240 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Type	Description
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

Query details about a network ACL.

```
GET https://{Endpoint}/v3/{project_id}/vpc/firewalls/{firewall_id}
```

Example Response

Status code: 200

OK

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
    "updated_at" : "2022-04-07T07:30:46Z",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "ACTIVE",
    "tags" : [ ],
    "ingress_rules" : [ {
      "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
      "name" : "network_acl_rule test",
      "description" : "network_acl_rule test",
      "action" : "allow",
      "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
      "protocol" : "tcp",
```



```
    "ip_version" : 4,
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
   } ],
   "egress_rules" : [ {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_rule test",
    "description" : "network_acl_rule test",
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
   } ],
   "associations" : [ {
    "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
   } ]
  }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.4 Updating a Network ACL

Function

This API is used to update a network ACL.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}

Table 5-241 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique identifier of a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

Table 5-242 Request body parameter

Parameter	Mandatory	Type	Description
firewall	Yes	**UpdateFirewallOption** object	Request body for updating a network ACL.

Table 5-243 UpdateFirewallOption

Parameter	Mandatory	Type	Description
name	No	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	Provides supplementary information about the IP address group. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
admin_state_up	No	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.

Response Parameters

Status code: 200

Table 5-244 Response body parameters

Parameter	Type	Description
firewall	**FirewallDetail** object	Response body for updating a network ACL
request_id	String	Request ID

Table 5-245 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about the IP address group. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.

Parameter	Type	Description
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-246 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-247 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-248 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Type	Description
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

Change the name and description of the network ACL e9a7731d-5bd9-4250-a524-b9a076fd5629 to **network_acl_test1** and enable the network ACL.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/firewalls/{firewall_id}

{
    "firewall": {
        "name": "network_acl_test1",
        "description": "network_acl_test1",
        "admin_state_up": true
    }
}
```

Example Response

Status code: 200

OK

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
    "updated_at" : "2022-04-07T07:30:46Z",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "ACTIVE",
    "tags" : [ ],
    "ingress_rules" : [ {
      "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
      "name" : "network_acl_rule test",
      "description" : "network_acl_rule test",
      "action" : "allow",
      "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
```



```
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
   } ],
   "egress_rules" : [ {
    "id" : "f9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_rule test",
    "description" : "network_acl_rule test",
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
   } ],
   "associations" : [ {
    "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
   } ]
  }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.5 Deleting a Network ACL

Function

This API is used to delete a network ACL.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

DELETE /v3/{project_id}/vpc/firewalls/{firewall_id}

Table 5-249 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique identifier of a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

None

Response Parameters

None

Example Request

Delete a network ACL.

```
DELETE https://{Endpoint}/v3/{project_id}/vpc/firewalls/{firewall_id}
```

Example Response

None

Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.6 Updating a Network ACL Rule

Function

This API is used to update a network ACL rule.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/update-rules

Table 5-250 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique identifier of a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

Table 5-251 Request body parameter

Parameter	Mandatory	Type	Description
firewall	Yes	**FirewallUpdateRuleOption** object	Update an inbound or outbound network ACL rule.

Table 5-252 FirewallUpdateRuleOption

Parameter	Mandatory	Type	Description
ingress_rules	No	Array of **FirewallUpdateRuleItemOption** objects	Update inbound network ACL rules. **ingress_rules** and **egress_rules** cannot be configured at the same time. Only one rule can be updated at a time.
egress_rules	No	Array of **FirewallUpdateRuleItemOption** objects	Update outbound network ACL rules. **ingress_rules** and **egress_rules** cannot be configured at the same time. Only one rule can be updated at a time.

Table 5-253 FirewallUpdateRuleItemOption

Parameter	Mandatory	Type	Description
id	Yes	String	Network ACL rule ID, which uniquely identifies a network ACL rule The value is a string in UUID format.
name	No	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Mandatory	Type	Description
description	No	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	No	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
protocol	No	String	Network ACL rule protocol. The value can be **tcp**, **udp**, **icmp**, **icmpv6**, or an IP protocol number (0–255). The value **any** indicates all protocols.
ip_version	No	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	No	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	No	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	No	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Mandatory	Type	Description
destination_port	No	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
source_address_group_id	No	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	No	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	No	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Response Parameters

Status code: 200

Table 5-254 Response body parameters

Parameter	Type	Description
firewall	**FirewallDetail** object	Details after a network ACL rule is updated.
request_id	String	Request ID.

Table 5-255 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about an IP address group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.

Parameter	Type	Description
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-256 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-257 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-258 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Type	Description
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

Update the inbound rule e9a7731d-5bd9-4250-a524-b9a076fd5629 in the network ACL e9a7731d-5bd9-4250-a524-b9a076fd5629.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/firewalls/e9a7731d-5bd9-4250-a524-b9a076fd5629/update-rules

{
  "firewall" : {
    "ingress_rules" : [ {
      "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
      "name" : "network_acl_rule test2",
      "description" : "network_acl_rule test2",
      "action" : "allow",
      "protocol" : "tcp",
      "ip_version" : "4",
      "source_ip_address" : "192.168.3.0/24",
      "destination_ip_address" : "192.168.6.0/24",
      "source_port" : "30-40,60-90",
      "destination_port" : "40-60,70-90",
      "source_address_group_id" : null,
      "destination_address_group_id" : null
    } ]
  }
}
```

Example Response

Status code: 200

OK

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
```



```
  "updated_at" : "2022-04-07T07:30:46Z",
  "admin_state_up" : true,
  "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
  "status" : "ACTIVE",
  "tags" : [ ],
  "ingress_rules" : [ {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_rule test2",
    "description" : "network_acl_rule test2",
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
  } ],
  "egress_rules" : [ {
    "id" : "f9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_rule test",
    "description" : "network_acl_rule test",
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
  } ],
  "associations" : [ {
    "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
  } ]
 }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.7 Inserting a Network ACL Rule

Function

This API is used to insert a network ACL rule.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/insert-rules

Table 5-259 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique identifier of a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

Table 5-260 Request body parameter

Parameter	Mandatory	Type	Description
firewall	Yes	**FirewallInsertRuleOption** object	Insert inbound and outbound network ACL rules.

Table 5-261 FirewallInsertRuleOption

Parameter	Mandatory	Type	Description
ingress_rules	No	Array of **FirewallInsertRuleItemOption** objects	Add inbound network ACL rules.
egress_rules	No	Array of **FirewallInsertRuleItemOption** objects	Add outbound network ACL rules.
insert_after_rule	No	String	Insert a network ACL rule below an inbound or outbound rule. If **insert_after_rule** is specified, **ingress_rules** and **egress_rules** cannot be configured at the same time, and the rule must exist in the inbound or outbound direction.

Table 5-262 FirewallInsertRuleItemOption

Parameter	Mandatory	Type	Description
name	No	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	No	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	Yes	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
protocol	Yes	String	Network ACL rule protocol. The value can be **tcp**, **udp**, **icmp**, **icmpv6**, or an IP protocol number (0–255). The value **any** indicates all protocols.
ip_version	Yes	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	No	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	No	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	No	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Mandatory	Type	Description
destination_port	No	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
source_address_group_id	No	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	No	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	No	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Response Parameters

Status code: 200

Table 5-263 Response body parameters

Parameter	Type	Description
firewall	**FirewallDetail** object	Details after a network ACL rule is inserted.
request_id	String	Request ID.

Table 5-264 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about an IP address group. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.

Parameter	Type	Description
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-265 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-266 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-267 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Type	Description
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

- Insert two inbound rules below the rule a2a7731d-5bd9-4250-a524-b9a076fd5630 to the network ACL e9a7731d-5bd9-4250-a524-b9a076fd5629.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/firewalls/e9a7731d-5bd9-4250-a524-b9a076fd5629/insert-rules

{
  "firewall" : {
    "ingress_rules" : [ {
      "name" : "network_acl_rule ipv4 test",
      "description" : "network_acl_rule ipv4 test",
      "action" : "allow",
      "protocol" : "tcp",
      "ip_version" : "4",
      "source_ip_address" : "192.168.3.0/24",
      "destination_ip_address" : "192.168.6.0/24",
      "source_port" : "30-40,60-90",
      "destination_port" : "40-60,70-90",
      "source_address_group_id" : null,
      "destination_address_group_id" : null
    },{
      "name" : "network_acl_rule ipv6 test",
      "description" : "network_acl_rule ipv6 test",
      "action" : "allow",
      "protocol" : "tcp",
      "ip_version" : "6",
      "source_ip_address" : "2002:50::44",
      "destination_ip_address" : "2002:51::44",
      "source_port" : "30-40,60-90",
      "destination_port" : "40-60,70-90",
      "source_address_group_id" : null,
      "destination_address_group_id" : null
    } ],
    "insert_after_rule" : "a2a7731d-5bd9-4250-a524-b9a076fd5630"
  }
}
```

- Insert two outbound rules below the rule a3a7731d-5bd9-4250-a524-b9a076fd5630 to the network ACL e9a7731d-5bd9-4250-a524-b9a076fd5629.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/firewalls/e9a7731d-5bd9-4250-a524-b9a076fd5629/insert-rules
```



```
{
  "firewall" : {
    "egress_rules" : [ {
      "name" : "network_acl_rule ipv4 test",
      "description" : "network_acl_rule ipv4 test",
      "action" : "allow",
      "protocol" : "tcp",
      "ip_version" : "4",
      "source_ip_address" : "192.168.3.0/24",
      "destination_ip_address" : "192.168.6.0/24",
      "source_port" : "30-40,60-90",
      "destination_port" : "40-60,70-90",
      "source_address_group_id" : null,
      "destination_address_group_id" : null
    },{
      "name" : "network_acl_rule ipv6 test",
      "description" : "network_acl_rule ipv6 test",
      "action" : "allow",
      "protocol" : "tcp",
      "ip_version" : "6",
      "source_ip_address" : "2002:50::44",
      "destination_ip_address" : "2002:51::44",
      "source_port" : "30-40,60-90",
      "destination_port" : "40-60,70-90",
      "source_address_group_id" : null,
      "destination_address_group_id" : null
    }],
    "insert_after_rule" : "a3a7731d-5bd9-4250-a524-b9a076fd5630"
  }
}
```

Example Response

Status code: 200

OK

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
    "updated_at" : "2022-04-07T07:30:46Z",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "ACTIVE",
    "tags" : [ ],
    "ingress_rules" : [{
      "id" : "a2a7731d-5bd9-4250-a524-b9a076fd5630",
      "name" : "network_acl_rule",
      "description" : "network_acl_rule",
      "action" : "allow",
      "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
      "protocol" : "tcp",
      "ip_version" : "4",
      "source_ip_address" : "192.168.13.0/24",
      "destination_ip_address" : "192.168.16.0/24",
      "source_port" : "30-40,60-90",
      "destination_port" : "40-60,70-90",
      "source_address_group_id" : null,
      "destination_address_group_id" : null
    },{
      "id" : "4afc959f-5380-dd94-8082-5701f6bc3f1c",
      "name" : "network_acl_rule ipv4 test",
      "description" : "network_acl_rule ipv4 test",
      "action" : "allow",
```



```
  "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
  "protocol" : "tcp",
  "ip_version" : "4",
  "source_ip_address" : "192.168.3.0/24",
  "destination_ip_address" : "192.168.6.0/24",
  "source_port" : "30-40,60-90",
  "destination_port" : "40-60,70-90",
  "source_address_group_id" : null,
  "destination_address_group_id" : null
},{
  "id" : "b49dcd4c-508e-4b99-9093-2680616f2a7e",
  "name" : "network_acl_rule ipv6 test",
  "description" : "network_acl_rule ipv6 test",
  "action" : "allow",
  "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
  "protocol" : "tcp",
  "ip_version" : "6",
  "source_ip_address" : "2002:50::44",
  "destination_ip_address" : "2002:51::44",
  "source_port" : "30-40,60-90",
  "destination_port" : "40-60,70-90",
  "source_address_group_id" : null,
  "destination_address_group_id" : null
}],
"egress_rules" : [{
  "id" : "a3a7731d-5bd9-4250-a524-b9a076fd5630",
  "name" : "network_acl_rule",
  "description" : "network_acl_rule",
  "action" : "allow",
  "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
  "protocol" : "tcp",
  "ip_version" : "4",
  "source_ip_address" : "192.168.13.0/24",
  "destination_ip_address" : "192.168.16.0/24",
  "source_port" : "30-40,60-90",
  "destination_port" : "40-60,70-90",
  "source_address_group_id" : null,
  "destination_address_group_id" : null
},{
  "id" : "f9a7731d-5bd9-4250-a524-b9a076fd5629",
  "name" : "network_acl_rule ipv4 test",
  "description" : "network_acl_rule ipv4 test",
  "action" : "allow",
  "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
  "protocol" : "tcp",
  "ip_version" : "4",
  "source_ip_address" : "192.168.3.0/24",
  "destination_ip_address" : "192.168.6.0/24",
  "source_port" : "30-40,60-90",
  "destination_port" : "40-60,70-90",
  "source_address_group_id" : null,
  "destination_address_group_id" : null
}, {
  "id" : "bbbc1cd1-b8e1-45d3-b3bc-7bc360f8860d",
  "name" : "network_acl_rule ipv6 test",
  "description" : "network_acl_rule ipv6 test",
  "action" : "allow",
  "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
  "protocol" : "tcp",
  "ip_version" : "6",
  "source_ip_address" : "2002:50::44",
  "destination_ip_address" : "2002:51::44",
  "source_port" : "30-40,60-90",
  "destination_port" : "40-60,70-90",
  "source_address_group_id" : null,
  "destination_address_group_id" : null
}],
"associations" : [ {
  "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
```



```
  }]
 }
}
```

Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.8 Deleting a Network ACL Rule

Function

This API is used to delete a network ACL rule.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/remove-rules

Table 5-268 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique identifier of a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

Table 5-269 Request body parameter

Parameter	Mandatory	Type	Description
firewall	Yes	**FirewallRemoveRuleOption** object	Inbound or outbound network ACL rules to be deleted.

Table 5-270 FirewallRemoveRuleOption

Parameter	Mandatory	Type	Description
ingress_rules	No	Array of **FirewallRemoveRuleItemOption** objects	Delete inbound network ACL rules. **ingress_rules** and **egress_rules** cannot be configured at the same time.
egress_rules	No	Array of **FirewallRemoveRuleItemOption** objects	Delete outbound network ACL rules. **ingress_rules** and **egress_rules** cannot be configured at the same time.

Table 5-271 FirewallRemoveRuleItemOption

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the network ACL rule to be deleted.

Response Parameters

Status code: 200

Table 5-272 Response body parameters

Parameter	Type	Description
firewall	**FirewallDetail** object	Details after a network ACL rule is deleted.
request_id	String	Request ID.

Table 5-273 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.

Parameter	Type	Description
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about an IP address group. The value can contain no more than 255 characters and cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.

Parameter	Type	Description
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-274 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-275 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-276 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).

Parameter	Type	Description
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.

Parameter	Type	Description
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

Delete the inbound rule e9a7731d-5bd9-4250-a524-b9a076fd5629 from the network ACL e9a7731d-5bd9-4250-a524-b9a076fd5629.

```
PUT /v3/{project_id}/vpc/firewalls/e9a7731d-5bd9-4250-a524-b9a076fd5629/remove-rules

{
  "firewall" : {
    "ingress_rules" : [ {
      "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629"
    } ]
  }
}
```

Example Response

Status code: 200

OK

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
    "updated_at" : "2022-04-07T07:30:46Z",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "ACTIVE",
    "tags" : [ ],
    "ingress_rules" : [ ],
    "egress_rules" : [ {
      "id" : "f9a7731d-5bd9-4250-a524-b9a076fd5629",
      "name" : "network_acl_rule test",
      "description" : "network_acl_rule test",
      "action" : "allow",
      "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
      "protocol" : "tcp",
      "ip_version" : "4",
      "source_ip_address" : "192.168.3.0/24",
      "destination_ip_address" : "192.168.6.0/24",
      "source_port" : "30-40,60-90",
      "destination_port" : "40-60,70-90",
      "source_address_group_id" : null,
      "destination_address_group_id" : null
    } ],
    "associations" : [ {
      "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
    } ]
  }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.9 Associating a Subnet with a Network ACL

Function

This API is used to associate a subnet with a network ACL.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/associate-subnets

Table 5-277 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique identifier of a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

Table 5-278 Request body parameter

Parameter	Mandatory	Type	Description
subnets	Yes	Array of **FirewallAssociation** objects	Subnets associated with a network ACL.

Table 5-279 FirewallAssociation

Parameter	Mandatory	Type	Description
virsubnet_id	Yes	String	ID of a subnet that is associated with a network ACL.

Response Parameters

Status code: 200

Table 5-280 Response body parameters

Parameter	Type	Description
firewall	FirewallDetail object	Response body for associating a subnet with a network ACL.
request_id	String	Request ID.

Table 5-281 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about an IP address group. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.

Parameter	Type	Description
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-282 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-283 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-284 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Type	Description
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

Associate the subnet 8359e5b0-353f-4ef3-a071-98e67a34a143 with the network ACL e9a7731d-5bd9-4250-a524-b9a076fd5629.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/firewalls/e9a7731d-5bd9-4250-a524-b9a076fd5629/associate-subnets

{
  "subnets" : [ {
    "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
  } ]
}
```

Example Response

Status code: 200

OK

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
    "updated_at" : "2022-04-07T07:30:46Z",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "ACTIVE",
```



```
  "tags" : [ ],
  "ingress_rules" : [ {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_rule test",
    "description" : "network_acl_rule test",
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : 4,
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
  } ],
  "egress_rules" : [ {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_rule test",
    "description" : "network_acl_rule test",
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
  } ],
  "associations" : [ {
    "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
  } ]
 }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.9.10 Disassociating a Subnet from a Network ACL

Function

This API is used to disassociate a subnet from a network ACL.

This API is now available in CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Singapore.

URI

PUT /v3/{project_id}/vpc/firewalls/{firewall_id}/disassociate-subnets

Table 5-285 Parameter description

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	Unique identifier of a network ACL.
project_id	Yes	String	Project ID.

Request Parameters

Table 5-286 Request body parameter

Parameter	Mandatory	Type	Description
subnets	Yes	Array of **FirewallAssociation** objects	Subnets disassociated from a network ACL.

Table 5-287 FirewallAssociation

Parameter	Mandatory	Type	Description
virsubnet_id	Yes	String	ID of a subnet that is associated with a network ACL.

Response Parameters

Status code: 200

Table 5-288 Response body parameters

Parameter	Type	Description
firewall	**FirewallDetail** object	Response body for disassociating a subnet from a network ACL.
request_id	String	Request ID.

Table 5-289 FirewallDetail

Parameter	Type	Description
id	String	Network ACL ID, which uniquely identifies a network ACL. The value is a string in UUID format.
name	String	Network ACL name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).
description	String	Provides supplementary information about an IP address group. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
project_id	String	ID of the project that a network ACL belongs to.
created_at	String	Time when a network ACL is created UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
updated_at	String	Time when a network ACL was last updated UTC time in the format of yyyy-MM-ddTHH:mmssZ. The value is automatically generated by the system.
admin_state_up	Boolean	Whether a network ACL is enabled. The value can be **true** or **false**. **true** indicates that the network ACL is enabled, and **false** indicates that the network ACL is disabled.
status	String	Network ACL status.
enterprise_project_id	String	ID of the enterprise project that a network ACL belongs to. The value is **0** or a string that contains a maximum of 36 characters in UUID format with hyphens (-). Value **0** indicates the default enterprise project.
tags	Array of **ResourceTag** objects	Network ACL tags.

Parameter	Type	Description
associations	Array of **FirewallAssociation** objects	Subnets that are associated with a network ACL.
ingress_rules	Array of **FirewallRuleDetail** objects	Inbound network ACL rules.
egress_rules	Array of **FirewallRuleDetail** objects	Outbound network ACL rules.

Table 5-290 ResourceTag

Parameter	Type	Description
key	String	Tag key. Tag keys must be unique for each resource. Minimum length: **1** Maximum length: **128**
value	String	Tag value. Maximum length: **255**

Table 5-291 FirewallAssociation

Parameter	Type	Description
virsubnet_id	String	IDs of subnets that are associated with a network ACL.

Table 5-292 FirewallRuleDetail

Parameter	Type	Description
id	String	Network ACL rule ID, which uniquely identifies a network ACL rule. The value is a string in UUID format.
name	String	Network ACL rule name. The value can contain no more than 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Type	Description
description	String	Provides supplementary information about a network ACL rule. The value can contain no more than 255 characters. The value cannot contain angle brackets (< or >).
action	String	Whether a network ACL rule allows or denies traffic. The value can be **allow** or **deny**.
project_id	String	ID of the project that a network ACL belongs to.
protocol	String	Network ACL rule protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPV6**, or a value from 0 to 255.
ip_version	Integer	IP version of a network ACL rule. The value can be **4** (IPv4) or **6** (IPv6).
source_ip_address	String	Source IP address or CIDR block of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_ip_address	String	Destination IP address or CIDR block of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
source_port	String	Source ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.
destination_port	String	Destination ports of a network ACL rule. You can specify a single port or a port range. Separate every two entries with a comma. The default number of supported port entries is 20.

Parameter	Type	Description
source_address_group_id	String	Source IP address group ID of a network ACL rule. **source_ip_address** and **source_address_group_id** cannot be configured at the same time.
destination_address_group_id	String	Destination IP address group ID of a network ACL rule. **destination_ip_address** and **destination_address_group_id** cannot be configured at the same time.
enabled	Boolean	Whether to enable a network ACL rule. The value can be **true** (enabled) or **false** (disabled). Default value: **true**

Example Request

Disassociate subnets 8359e5b0-353f-4ef3-a071-98e67a34a143 and d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163 from the network ACL e9a7731d-5bd9-4250-a524-b9a076fd5629.

```
PUT https://{Endpoint}/v3/{project_id}/vpc/firewalls/e9a7731d-5bd9-4250-a524-b9a076fd5629/disassociate-subnets

{
  "subnets" : [ {
    "virsubnet_id" : "8359e5b0-353f-4ef3-a071-98e67a34a143"
  }, {
    "virsubnet_id" : "d9994dcf-ef6d-47ec-9ac9-a62d4fd5e163"
  } ]
}
```

Example Response

Status code: 200

OK

```
{
  "firewall" : {
    "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_test1",
    "description" : "network_acl_test1",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "created_at" : "2022-04-07T07:30:46Z",
    "updated_at" : "2022-04-07T07:30:46Z",
    "admin_state_up" : true,
    "enterprise_project_id" : "158ad39a-dab7-45a3-9b5a-2836b3cf93f9",
    "status" : "INACTIVE",
    "tags" : [ ],
    "ingress_rules" : [ {
      "id" : "e9a7731d-5bd9-4250-a524-b9a076fd5629",
      "name" : "network_acl_rule test",
      "description" : "network_acl_rule test",
```



```
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
   } ],
   "egress_rules" : [ {
    "id" : "f9a7731d-5bd9-4250-a524-b9a076fd5629",
    "name" : "network_acl_rule test",
    "description" : "network_acl_rule test",
    "action" : "allow",
    "project_id" : "9476ea5a8a9849c38358e43c0c3a9e12",
    "protocol" : "tcp",
    "ip_version" : "4",
    "source_ip_address" : "192.168.3.0/24",
    "destination_ip_address" : "192.168.6.0/24",
    "source_port" : "30-40,60-90",
    "destination_port" : "40-60,70-90",
    "source_address_group_id" : null,
    "destination_address_group_id" : null
   } ],
   "associations" : [ ]
  }
}
```


Status Codes

See **Status Codes**.

Error Codes

See **Error Codes**.

5.10 Network ACL Tag Management

5.10.1 Querying the Number of Network ACLs Using Tags

Function

This API is used to query the number of network ACLs using tags.

URI

POST /v3/{project_id}/firewalls/resource-instances/count

Table 5-293 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 5-294 Request body parameters

Parameter	Mandatory	Type	Description
matches	No	Array of **Match** objects	The key-value pair to be matched in the query. The key is a fixed dictionary value and must be a unique and supported key. The key can only be resource_name.
tags	No	Array of **ListTag** objects	The resources to be queried contain all tags listed in tags. A maximum of 50 tags can be specified. Each tag key can have a maximum of 10 tag values. Each tag value can be an empty array but the structure cannot be missing. Each tag key must be unique, and each tag value of a tag must also be unique. Resources with all tags listed in tags will be returned. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If tags is not specified, all resources will be returned.

Table 5-295 Match

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Currently, the tag key can only be the resource name. Maximum length: 128 Minimum: **1** Maximum: **128**
value	Yes	String	Tag value. Each value can contain a maximum of 255 Unicode characters. Maximum length: 255 Minimum: **0** Maximum: **255**

Table 5-296 ListTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key The key cannot be left blank. Maximum length: 128 Minimum: **1** Maximum: **128**
values	Yes	Array of strings	Tag values. If values is left blank, it indicates any_value (querying any value). The values are in the OR relationship. Maximum length: 255 Maximum: **255**

Response Parameters

Status code: 200

Table 5-297 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
total_count	Integer	Resource quantity

Status code: 400

Table 5-298 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-299 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-300 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 404

Table 5-301 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-302 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Query network ACLs using tags and matches.


```
POST https://{{Endpoint}}/v3/{project_id}/firewalls/resource-instances/count

{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1" ]
  } ],
  "matches" : [ {
    "key" : "resource_name",
    "value" : "network_aclv3_test"
  } ]
}
```

Example Responses

Status code: 200

Normal request response

```
{
  "request_id" : "239df34e-a651-4631-aaa1-d5fef231933a",
  "total_count" : 2
}
```

Status Codes

Status Code	Description
200	Normal request response
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found
500	System exception

Error Codes

See **Error Codes**.

5.10.2 Querying Network ACLs Using Tags

Function

This API is used to query network ACLs using tags.

URI

POST /v3/{project_id}/firewalls/resource-instances/filter

Table 5-303 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 5-304 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records to be queried The value can be from 1 to 1000. The default value is 1000. Default: **1000**
offset	No	Integer	The index position. The query starts from the next piece of data indexed by this parameter. The value is 0 by default, indicating that the query starts from the first piece of data. The value cannot be a negative number. Default: **0**

Request Parameters

Table 5-305 Request body parameters

Parameter	Mandatory	Type	Description
matches	No	Array of **Match** objects	The key-value pair to be matched in the query.The key is a fixed dictionary value and must be a unique and supported key. The key can only be resource_name.

Parameter	Mandatory	Type	Description
tags	No	Array of **ListTag** objects	The resources to be queried contain all tags listed in tags. A maximum of 50 tags can be specified. Each tag key can have a maximum of 10 tag values. Each tag value can be an empty array but the structure cannot be missing. Each tag key must be unique, and each tag value of a tag must also be unique.Resources with all tags listed in tags will be returned. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If tags is not specified, all resources will be returned.

Table 5-306 Match

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. Currently, the tag key can only be the resource name. Maximum length: 128 Minimum: **1** Maximum: **128**
value	Yes	String	Tag value. Each value can contain a maximum of 255 Unicode characters. Maximum length: 255 Minimum: **0** Maximum: **255**

Table 5-307 ListTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key The key cannot be left blank. Maximum length: 128 Minimum: **1** Maximum: **128**
values	Yes	Array of strings	Tag values. If values is left blank, it indicates any_value (querying any value). The values are in the OR relationship. Maximum length: 255 Maximum: **255**

Response Parameters

Status code: 200

Table 5-308 Response body parameters

Parameter	Type	Description
resources	Array of **ListResourceResp** objects	Resources
total_count	Integer	Resource quantity
request_id	String	Request ID

Table 5-309 ListResourceResp

Parameter	Type	Description
resource_id	String	Resource ID
resource_detail	Object	Resource details that are used for extension. This parameter is left blank by default.
resource_name	String	Resource name. This parameter is an empty string by default if there is no resource name.
tags	Array of **ResourceTag** objects	A list of tags for queried resources to match against. This parameter is an empty array by default if there is no tag.

Table 5-310 ResourceTag

Parameter	Type	Description
key	String	Tag key Tag keys must be unique for each resource. Maximum length: 128 Minimum: **1** Maximum: **128**
value	String	Tag value Maximum length: 255 Maximum: **255**

Status code: 400

Table 5-311 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-312 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-313 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message

Parameter	Type	Description
error_code	String	Error code

Status code: 404

Table 5-314 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-315 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Query network ACLs using tags and matches. A maximum of 100 records can be returned. The query starts from the first record.

```
https://{{Endpoint}}/v3/{project_id}/firewalls/resource-instances/filter?limit=100&offset=0

{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1" ]
  } ],
  "matches" : [ {
    "key" : "resource_name",
    "value" : "network_aclv3_test"
  } ]
}
```

Example Responses

Status code: 200

Normal request response

```
{
  "resources" : [ {
```



```
    "resource_id" : "55046c0b-f38e-4bc4-988a-06529b34a7db",
    "resource_detail" : "",
    "resource_name" : "network_aclv3_test",
    "tags" : [ {
      "key" : "key1",
      "value" : "value1"
    }, {
      "key" : "key2",
      "value" : "value2"
    } ]
  }, {
    "resource_id" : "1828c600-793d-4570-987b-ac59f3ef0734",
    "resource_detail" : "",
    "resource_name" : "network_aclv3_test",
    "tags" : [ {
      "key" : "key1",
      "value" : "value1"
    }, {
      "key" : "key5",
      "value" : "value5"
    } ]
  } ],
  "request_id" : "2d9cef8c-4e17-40bc-9111-f3fc97b97294",
  "total_count" : 2
}
```


Status Codes

Status Code	Description
200	Normal request response
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found
500	System exception

Error Codes

See **Error Codes**.

5.10.3 Adding a Tag to a Network ACL

Function

This API is used to add a tag to a specific network ACL. This is an idempotent API. If the new tag has the same key as an existing tag, the tag will be created and overwrite the existing one.

URI

POST /v3/{project_id}/firewalls/{firewall_id}/tags

Table 5-316 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	The unique ID of a network ACL. The value is a string in UUID format. The network ACL with a given ID must exist.
project_id	Yes	String	Project ID

Request Parameters

Table 5-317 Request body parameters

Parameter	Mandatory	Type	Description
tag	Yes	**ResourceTag** object	Request body for adding tags to a network ACL

Table 5-318 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key Tag keys must be unique for each resource. Maximum length: 128 Minimum: **1** Maximum: **128**
value	Yes	String	Tag value Maximum length: 255 Maximum: **255**

Response Parameters

Status code: 400

Table 5-319 Response body parameters

Parameter	Type	Description
request_id	String	Request ID

Parameter	Type	Description
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-320 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-321 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 404

Table 5-322 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-323 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Add a tag to a network ACL. Set the tag key to key4 and tag value to value4.

```
POST https://{Endpoint}/v3/{project_id}/firewalls/{firewall_id}/tags

{
  "tag" : {
    "key" : "key4",
    "value" : "value4"
  }
}
```

Example Responses

None

Status Codes

Status Code	Description
204	Normal request response
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found
500	System exception

Error Codes

See **Error Codes**.

5.10.4 Delete a Tag from a Network ACL

Function

This API is used to delete a tag from a specified network ACL. This is an idempotent API. The tag key cannot be left blank or be an empty string. If the key of the tag to be deleted does not exist, 404 will be returned.

URI

DELETE /v3/{project_id}/firewalls/{firewall_id}/tags/{tag_key}

Table 5-324 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	The unique ID of a network ACL. The value is a string in UUID format. The network ACL with a given ID must exist.
project_id	Yes	String	Project ID
tag_key	Yes	String	Tag key

Request Parameters

None

Response Parameters

Status code: 400

Table 5-325 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-326 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-327 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 404

Table 5-328 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-329 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Delete a tag from a network ACL.


```
DELETE https://{Endpoint}/v3/{project_id}/firewalls/{firewall_id}/tags/{tag_key}
```

Example Responses

None

Status Codes

Status Code	Description
204	Normal request response
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found
500	System exception

Error Codes

See **Error Codes**.

5.10.5 Querying Tags of Network ACLs

Function

This API is used to query tags of a specific network ACL.

URI

GET /v3/{project_id}/firewalls/{firewall_id}/tags

Table 5-330 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	The unique ID of a network ACL. The value is a string in UUID format. The network ACL with a given ID must exist.
project_id	Yes	String	Project ID

Request Parameters

None

Response Parameters

Status code: 200

Table 5-331 Response body parameters

Parameter	Type	Description
tags	Array of **ResourceTag** objects	Tags
request_id	String	Request ID

Table 5-332 ResourceTag

Parameter	Type	Description
key	String	Tag key Tag keys must be unique for each resource. Maximum length: 128 Minimum: **1** Maximum: **128**
value	String	Tag value Maximum length: 255 Maximum: **255**

Status code: 400

Table 5-333 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-334 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-335 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 404

Table 5-336 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-337 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Query tags of a network ACL.


```
GET https://{Endpoint}/v3/{project_id}/firewalls/{firewall_id}/tags
```

Example Responses

Status code: 200

Normal response to the GET operation

```
{
  "request_id" : "95cedc2b-4b3d-4e5c-af29-74576daf5513",
  "tags" : [ {
    "key" : "key5",
    "value" : "value5"
  }, {
    "key" : "key1",
    "value" : "value1"
  } ]
}
```

Status Codes

Status Code	Description
200	Normal response to the GET operation
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found
500	System exception

Error Codes

See **Error Codes**.

5.10.6 Adding Tags to a Network ACL in Batches

Function

This API is used to add tags to a specified network ACL in batches. This is an idempotent API. When you add tags, if there are duplicate keys in the request body, an error is reported. Duplicate keys are not allowed. If a key already exists, its value will be overwritten by the new value.

URI

POST /v3/{project_id}/firewalls/{firewall_id}/tags/create

Table 5-338 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	The unique ID of a network ACL. The value is a string in UUID format. The network ACL with a given ID must exist.
project_id	Yes	String	Project ID

Request Parameters

Table 5-339 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of **ResourceTag** objects	Tags

Table 5-340 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key Tag keys must be unique for each resource. Maximum length: 128 Minimum: **1** Maximum: **128**
value	Yes	String	Tag value Maximum length: 255 Maximum: **255**

Response Parameters

Status code: 400

Table 5-341 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-342 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-343 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 404

Table 5-344 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-345 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Add two tags to a network ACL. For one tag, the key is keyxxx and the value is value1. The key of the other tag is keyyyy, and the value is value2.

```
POST https://{Endpoint}/v3/{project_id}/firewalls/{firewall_id}/tags/create

{
  "tags" : [ {
    "key" : "keyxxx",
    "value" : "value1"
  }, {
    "key" : "keyyyy",
    "value" : "value2"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
204	Normal request response
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found
500	System exception

Error Codes

See **Error Codes**.

5.10.7 Deleting Tags from a Network ACL in Batches

Function

This API is used to delete tags from a specified network ACL in batches. This is an idempotent API. If some tags to be deleted do not exist, the deletion is considered to be successful by default. The character set of the tags will not be checked. When you delete tags, the tag structure cannot be missing, and the key cannot be left blank or be an empty string.

URI

POST /v3/{project_id}/firewalls/{firewall_id}/tags/delete

Table 5-346 Path Parameters

Parameter	Mandatory	Type	Description
firewall_id	Yes	String	The unique ID of a network ACL. The value is a string in UUID format. The network ACL with a given ID must exist.
project_id	Yes	String	Project ID

Request Parameters

Table 5-347 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of **DeleteResourceTagRequestBody** objects	Tags

Table 5-348 DeleteResourceTagRequestBody

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. The key of the same resource must be unique. Minimum: **1** Maximum: **128**

Parameter	Mandatory	Type	Description
value	No	String	Tag key Maximum: **255**

Response Parameters

Status code: 400

Table 5-349 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-350 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-351 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 404

Table 5-352 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-353 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Delete tags from a network ACL in batches. The key of the tag is keyxxx, and the value is value1.

```
POST https://{Endpoint}/v3/{project_id}/firewalls/{firewall_id}/tags/delete

{
  "tags" : [ {
    "key" : "keyxxx",
    "value" : "value1"
  } ]
}
```

Example Responses

None

Status Codes

Status Code	Description
204	Normal request response
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found

Status Code	Description
500	System exception

Error Codes

See **Error Codes**.

5.10.8 Querying Tags of Network ACLs in a Project

Function

This API is used to query all tags of network ACLs in a specific project.

URI

GET /v3/{project_id}/firewalls/tags

Table 5-354 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 5-355 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of records to be queried Minimum: **1** Maximum: **1000** Default: **1000**
offset	No	Integer	The index position. The query starts from the next piece of data indexed by this parameter. The value is 0 by default, indicating that the query starts from the first piece of data. The value cannot be a negative number. Default: **0**

Request Parameters

None

Response Parameters

Status code: 200

Table 5-356 Response body parameters

Parameter	Type	Description
tags	Array of **ListTag** objects	Tags
request_id	String	Request ID
total_count	Integer	Resource quantity

Table 5-357 ListTag

Parameter	Type	Description
key	String	Tag key The key cannot be left blank. Maximum length: 128 Minimum: **1** Maximum: **128**
values	Array of strings	Tag values. If values is left blank, it indicates any_value (querying any value). The values are in the OR relationship. Maximum length: 255 Maximum: **255**

Status code: 400

Table 5-358 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 401

Table 5-359 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 403

Table 5-360 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 404

Table 5-361 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Status code: 500

Table 5-362 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
error_msg	String	Error message
error_code	String	Error code

Example Requests

Query tags of network ACLs by project ID.

```
GET https://{Endpoint}/v3/{project_id}/firewalls/tags
```

Example Responses

Status code: 200

Normal response to the operation

```
{
  "request_id" : "65ae533b-f32c-49df-9b5d-e55eda8f2c25",
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  }, {
    "key" : "key2",
    "values" : [ "value2" ]
  }, {
    "key" : "key3",
    "values" : [ "value3" ]
  }, {
    "key" : "key4",
    "values" : [ "value4" ]
  }, {
    "key" : "key5",
    "values" : [ "value5" ]
  }, {
    "key" : "keyyyy",
    "values" : [ "value2" ]
  } ]
}
```

Status Codes

Status Code	Description
200	Normal response to the operation
400	Invalid parameter
401	Authentication failure
403	Insufficient permissions
404	Not found
500	System exception

Error Codes

See **Error Codes**.

5.11 Ports

5.11.1 Adding a Security Group to a Security Group List of a Port

Function

This API is used to add a security group to a security group list of a port.

URI

PUT /v3/{project_id}/ports/{port_id}/insert-security-groups

Table 5-363 Parameter description

Parameter	Mandatory	Type	Description
port_id	Yes	String	Unique identifier of a port
project_id	Yes	String	Project ID

Request Parameters

Table 5-364 Request body parameter

Parameter	Mandatory	Type	Description
port	Yes	InsertSecurityGroupOption object	Request body for adding a security group to a security group list of a port

Table 5-365 InsertSecurityGroupOption

Parameter	Mandatory	Type	Description
security_groups	Yes	Array of strings	Security group IDs, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]

Parameter	Mandatory	Type	Description
index	No	Integer	Position that a security group is added to. The value starts from **0**. Example: 1. To add a security group to the first of the associated security group list, set **index** to **0**. 2. To add a security group after the *n*th security group in the associated security group list, set **index** to *n*. By default, a security group is added to the end of the security group list associated with the port.

Response Parameters

Status code: 200

Table 5-366 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
port	**port** object	Response body for adding a security group to a security group list of a port

Table 5-367 port

Parameter	Type	Description
admin_state_up	Boolean	• Administrative state • The value can be **true**. • Constraints: N/A • Default value: **true** • Permissions: N/A

Parameter	Type	Description
binding:host_id	String	• Host ID • Value range: N/A • This parameter is visible only to administrators. • Default value: N/A • Permissions: N/A
binding:profile	Object	• User-defined settings • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
binding:vif_details	Object	• VIF details. Parameter **ovs_hybrid_plug** specifies whether the OVS/bridge hybrid mode is used. • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
binding:vif_type	String	• Interface type of the port. The value can be **ovs**, **hw_veb**, or others. This is an extended attribute. • Value range: N/A • This parameter is visible only to administrators. • Default value: N/A • Permissions: N/A
binding:vnic_type	String	• Type of the bound vNIC. **normal** indicates software switching. **direct** indicates SR-IOV PCIe passthrough, which is not supported. • The value can be **normal** or **direct**. • Constraints: N/A • Default value: N/A • Permissions: N/A
created_at	String	• Time when a port is created • The value is a UTC time in the format of yyyy-MM-ddTHH:mmss. • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
updated_at	String	• Time when a port is updated. • The value is a UTC time in the format of yyyy-MM-ddTHH:mmss. • Constraints: N/A • Default value: N/A • Permissions: N/A
description	String	• Supplementary information about a port • The value can contain no more than 255 characters and cannot contain angle brackets (< or >). • Constraints: N/A • Default value: N/A • Permissions: N/A
device_id	String	• ID of the device that a port belongs to. • The value must be in standard UUID format. • The system automatically sets this parameter. • Default value: N/A • Permissions: N/A
device_owner	String	• Belonged device, which can be a DHCP server, router, load balancer, or Nova. • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
ecs_flavor	String	• Flavor of the ECS that the port belongs to • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
id	String	• Unique identifier of a port • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
instance_id	String	• ID of the instance that the port belongs to, for example, RDS instance ID. • Value range: N/A • The system automatically sets this parameter. • Default value: N/A • Permissions: N/A
instance_type	String	• Type of the instance that the port belongs to, for example, RDS. • Value range: N/A • The system automatically sets this parameter. • Default value: N/A • Permissions: N/A
mac_address	String	• MAC address • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
name	String	• Port name • The value can contain no more than 255 characters. This parameter is left blank by default. • Constraints: N/A • Default value: N/A • Permissions: N/A
port_security_enabled	Boolean	• Whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect. • The value can be **true** or **false**. • Constraints: N/A • Default value: N/A • Permissions: N/A
private_ips	Array of **PrivateIpInfo** objects	• Private IP address of the port • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
project_id	String	• Project ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
security_groups	Array of strings	• Security group • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
status	String	• Port status • The value can be **ACTIVE**, **BUILD**, or **DOWN**. • Constraints: N/A • Default value: N/A • Permissions: N/A
tenant_id	String	• Tenant ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
virsubnet_id	String	• Network ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
vpc_id	String	• VPC ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
vpc_tenant_id	String	• VPC tenant ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
vtep_ip	String	• VTEP IP address • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
enable_efi	Boolean	• Whether to enable **efi**. If **efi** is enabled, the port supports vRoCE. • The value can be **true** or **false**. • Constraints: N/A • Default value: **false** • Permissions: N/A
scope	String	• Application scope • The value can be **center** or **{azId}**. **center** indicates that the scope is the center. **{azId}** indicates that the scope is a specific AZ. • Constraints: N/A • Default value: **center** • Permissions: N/A
zone_id	String	• AZ that the port belongs to • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
binding:migration_info	Object	• Destination node information, including **binding:vif_details** and **binding:vif_type** • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
extra_dhcp_opts	Array of objects	• Extended attributes of DHCP • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
position_type	String	• Location type in the edge scenario • Value range: N/A • Constraints: N/A • Default value: **center** • Permissions: N/A
instance_info	Object	• Information about the instance bound to the port • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
tags	Array of strings	• Port tags • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
allowed_address_pairs	Array of **AllowAddressPair** objects	• A set of zero or more allowed address pairs. An address pair consists of an IP address and a MAC address. • Value range: N/A • Constraints: The IP address cannot be **0.0.0.0/0**. Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. Set **allowed_address_pairs** of the cloud server NIC to **1.1.1.1/0**. • Default value: N/A • Permissions: N/A

Table 5-368 PrivateIpInfo

Parameter	Type	Description
ip_address	String	Port IP address
subnet_cidr_id	String	ID of the device that a port belongs to.

Table 5-369 AllowAddressPair

Parameter	Type	Description
ip_address	String	IP address. You cannot set it to **0.0.0.0**. Configure an independent security group for the port if parameter **allowed_address_pairs** has a CIDR block with a netmask length less than 24.
mac_address	String	MAC address

Example Request

Add a security group after the first security group (**567be4e3-d171-46ce-9e8a-c15e91cfe86a**) to the security group list (**["567be4e3-d171-46ce-9e8a-c15e91cfe86a", "4940b983-5992-4663-bed9-d1d1e15d1009"]**) associated with the port (**99fd0c77-56b4-4bf6-8365-df352e45d5fc**). Set **index** to **1**.

```
PUT https://{Endpoint}/v3/f5dab68cd75740e68c599e9af5fe0aed/ports/99fd0c77-56b4-4bf6-8365-df352e45d5fc/insert-security-groups

{
  "port" : {
    "security_groups" : [ "8edd3747-ccd4-49a1-82b9-a165eec314b4", "6c2d4540-3b7d-4207-a319-a7231b439995" ],
    "index" : 1
  }
}
```

Example Response

Status code: 200

OK

```
{
  "port" : {
    "name" : "",
    "id" : "99fd0c77-56b4-4bf6-8365-df352e45d5fc",
    "admin_state_up" : true,
    "status" : "DOWN",
    "project_id" : "f5dab68cd75740e68c599e9af5fe0aed",
    "device_id" : "",
    "mac_address" : "fa:16:3e:1f:17:df",
    "device_owner" : "",
    "description" : "",
    "vpc_id" : null,
    "zone_id" : "",
    "scope" : "center",
    "position_type" : "center",
    "vtep_ip" : null,
    "created_at" : "2023-05-10T01:35:02",
    "updated_at" : "2023-05-10T01:35:02",
    "port_security_enabled" : true,
    "tags" : [ ],
    "security_groups" : [ "567be4e3-d171-46ce-9e8a-c15e91cfe86a", "8edd3747-ccd4-49a1-82b9-a165eec314b4", "6c2d4540-3b7d-4207-a319-a7231b439995", "4940b983-5992-4663-bed9-d1d1e15d1009" ],
    "allowed_address_pairs" : [ ],
    "extra_dhcp_opts" : [ ],
    "instance_info" : null,
```



```
    "instance_id" : "",
    "instance_type" : "",
    "ecs_flavor" : "",
    "enable_efi" : false,
    "virsubnet_id" : "3847b263-2370-45c0-8236-38a1de568049",
    "private_ips" : [ {
      "subnet_cidr_id" : "ffe98087-6d4f-45cd-988b-1c87f75d2d53",
      "ip_address" : "192.168.158.228"
    } ],
    "vpc_tenant_id" : null,
    "binding:host_id" : "",
    "binding:vif_type" : "unbound",
    "binding:vnic_type" : "normal",
    "binding:vif_details" : { },
    "binding:profile" : { },
    "binding:migration_info" : { }
  },
  "request_id" : "458691c0-7db2-43d8-9400-053800c5ff53"
}
```


Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Internal Server Error

Error Codes

See **Error Codes**.

5.11.2 Removing a Security Group from a Security Group List of a Port

Function

This API is used to remove a security group from a security group list of a port.

URI

PUT /v3/{project_id}/ports/{port_id}/remove-security-groups

Table 5-370 Parameter description

Parameter	Mandatory	Type	Description
port_id	Yes	String	Unique identifier of a port
project_id	Yes	String	Project ID

Request Parameters

Table 5-371 Request body parameter

Parameter	Mandatory	Type	Description
port	Yes	**RemoveSecurityGroupOption** object	Request body for removing a security group from a security group list of a port

Table 5-372 RemoveSecurityGroupOption

Parameter	Mandatory	Type	Description
security_groups	Yes	Array of strings	Security group IDs Example: "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]

Response Parameters

Status code: 200

Table 5-373 Response body parameters

Parameter	Type	Description
request_id	String	Request ID
port	**port** object	Response body for removing a security group from a security group list of a port

Table 5-374 port

Parameter	Type	Description
admin_state_up	Boolean	• Administrative state • The value can be **true**. • Constraints: N/A • Default value: **true** • Permissions: N/A
binding:host_id	String	• Host ID • Value range: N/A • This parameter is visible only to administrators. • Default value: N/A • Permissions: N/A
binding:profile	Object	• User-defined settings • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
binding:vif_details	Object	• VIF details. Parameter **ovs_hybrid_plug** specifies whether the OVS/bridge hybrid mode is used. • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
binding:vif_type	String	• Interface type of the port. The value can be **ovs**, **hw_veb**, or others. This is an extended attribute. • Value range: N/A • This parameter is visible only to administrators. • Default value: N/A • Permissions: N/A
binding:vnic_type	String	• Type of the bound vNIC. **normal** indicates software switching. **direct** indicates SR-IOV PCIe passthrough, which is not supported. • The value can be **normal** or **direct**. • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
created_at	String	• Time when a port is created • The value is a UTC time in the format of yyyy-MM-ddTHH:mmss. • Constraints: N/A • Default value: N/A • Permissions: N/A
updated_at	String	• Time when a port is updated. • The value is a UTC time in the format of yyyy-MM-ddTHH:mmss. • Constraints: N/A • Default value: N/A • Permissions: N/A
description	String	• Supplementary information about a port • The value can contain no more than 255 characters and cannot contain angle brackets (< or >). • Constraints: N/A • Default value: N/A • Permissions: N/A
device_id	String	• ID of the device that a port belongs to. • The value must be in standard UUID format. • The system automatically sets this parameter. • Default value: N/A • Permissions: N/A
device_owner	String	• Belonged device, which can be a DHCP server, router, load balancer, or Nova. • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
ecs_flavor	String	• Flavor of the ECS that the port belongs to • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
id	String	• Unique identifier of a port • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
instance_id	String	• ID of the instance that the port belongs to, for example, RDS instance ID. • Value range: N/A • The system automatically sets this parameter. • Default value: N/A • Permissions: N/A
instance_type	String	• Type of the instance that the port belongs to, for example, RDS. • Value range: N/A • The system automatically sets this parameter. • Default value: N/A • Permissions: N/A
mac_address	String	• MAC address • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
name	String	• Port name • The value can contain no more than 255 characters. This parameter is left blank by default. • Constraints: N/A • Default value: N/A • Permissions: N/A
port_security_enabled	Boolean	• Whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect. • The value can be **true** or **false**. • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
private_ips	Array of **PrivateIpInfo** objects	• Private IP address of the port • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
project_id	String	• Project ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
security_groups	Array of strings	• Security group • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
status	String	• Port status • The value can be **ACTIVE**, **BUILD**, or **DOWN**. • Constraints: N/A • Default value: N/A • Permissions: N/A
tenant_id	String	• Tenant ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
virsubnet_id	String	• Network ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
vpc_id	String	• VPC ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
vpc_tenant_id	String	• VPC tenant ID • The value must be in standard UUID format. • Constraints: N/A • Default value: N/A • Permissions: N/A
vtep_ip	String	• VTEP IP address • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
enable_efi	Boolean	• Whether to enable **efi**. If **efi** is enabled, the port supports vRoCE. • The value can be **true** or **false**. • Constraints: N/A • Default value: **false** • Permissions: N/A
scope	String	• Application scope • The value can be **center** or **{azId}**. **center** indicates that the scope is the center. **{azId}** indicates that the scope is a specific AZ. • Constraints: N/A • Default value: **center** • Permissions: N/A
zone_id	String	• AZ that the port belongs to • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
binding:migration_info	Object	• Destination node information, including **binding:vif_details** and **binding:vif_type** • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A

Parameter	Type	Description
extra_dhcp_opts	Array of objects	• Extended attributes of DHCP • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
position_type	String	• Location type in the edge scenario • Value range: N/A • Constraints: N/A • Default value: **center** • Permissions: N/A
instance_info	Object	• Information about the instance bound to the port • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
tags	Array of strings	• Port tags • Value range: N/A • Constraints: N/A • Default value: N/A • Permissions: N/A
allowed_address_pairs	Array of **AllowAddressPair** objects	• A set of zero or more allowed address pairs. An address pair consists of an IP address and a MAC address. • Value range: N/A • Constraints: The IP address cannot be **0.0.0.0/0**. Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. Set **allowed_address_pairs** of the cloud server NIC to **1.1.1.1/0**. • Default value: N/A • Permissions: N/A

Table 5-375 FixedIp

Parameter	Type	Description
ip_address	String	Port IP address
subnet_id	String	ID of the device that a port belongs to.

Table 5-376 AllowAddressPair

Parameter	Type	Description
ip_address	String	IP address. You cannot set it to **0.0.0.0**. Configure an independent security group for the port if parameter **allowed_address_pairs** has a CIDR block with a netmask length less than 24.
mac_address	String	MAC address

Example Request

Remove security groups (**8edd3747-ccd4-49a1-82b9-a165eec314b4** and **6c2d4540-3b7d-4207-a319-a7231b439995**) associated with the port (**99fd0c77-56b4-4bf6-8365-df352e45d5fc**).

```
PUT https://{Endpoint}/v3/f5dab68cd75740e68c599e9af5fe0aed/ports/99fd0c77-56b4-4bf6-8365-df352e45d5fc/remove-security-groups

{
  "port" : {
    "security_groups" : [ "8edd3747-ccd4-49a1-82b9-a165eec314b4", "6c2d4540-3b7d-4207-a319-a7231b439995" ]
  }
}
```

Example Response

Status code: 200

OK

```
{
  "port" : {
    "name" : "",
    "id" : "99fd0c77-56b4-4bf6-8365-df352e45d5fc",
    "admin_state_up" : true,
    "status" : "DOWN",
    "project_id" : "f5dab68cd75740e68c599e9af5fe0aed",
    "device_id" : "",
    "mac_address" : "fa:16:3e:1f:17:df",
    "device_owner" : "",
    "description" : "",
    "vpc_id" : null,
    "zone_id" : "",
    "scope" : "center",
    "position_type" : "center",
    "vtep_ip" : null,
```



```
    "created_at" : "2023-05-10T01:35:02",
    "updated_at" : "2023-05-10T01:35:02",
    "port_security_enabled" : true,
    "tags" : [ ],
    "security_groups" : [ "567be4e3-d171-46ce-9e8a-c15e91cfe86a" ],
    "allowed_address_pairs" : [ ],
    "extra_dhcp_opts" : [ ],
    "instance_info" : null,
    "instance_id" : "",
    "instance_type" : "",
    "ecs_flavor" : "",
    "enable_efi" : false,
    "virsubnet_id" : "3847b263-2370-45c0-8236-38a1de568049",
    "private_ips" : [ {
      "subnet_cidr_id" : "ffe98087-6d4f-45cd-988b-1c87f75d2d53",
      "ip_address" : "192.168.158.228"
    } ],
    "vpc_tenant_id" : null,
    "binding:host_id" : "",
    "binding:vif_type" : "unbound",
    "binding:vnic_type" : "normal",
    "binding:vif_details" : { },
    "binding:profile" : { },
    "binding:migration_info" : { }
  },
  "request_id" : "abd08c76-c853-4967-a898-12804330efab"
}
```


Status Codes

Status Code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden
404	Not Found
409	Conflict
500	Internal Server Error

Error Codes

See **Error Codes**.

6 Native OpenStack Neutron APIs (V2.0)

6.1 API Version Information

6.1.1 Querying API Versions

Function

This API is used to query all available versions of a native OpenStack API.

URI

GET /

Request Parameters

None

Example Request

```
GET https://{Endpoint}/
```

Response Parameters

Table 6-1 Response parameter

Parameter	Type	Description
versions	Array of **version** objects	Specifies the API version list. For details, see **Table 6-2**.

Table 6-2 version objects

Parameter	Type	Description
status	String	Specifies the API version status. Possible values are as follows: • **CURRENT** • **STABLE** • **DEPRECATED**
id	String	Specifies the API version.
links	Array of **link** objects	Specifies the link list. For details, see **Table 6-3**.

Table 6-3 link objects

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

```
{
   "versions": [
      {
         "status": "CURRENT",
         "id": "v2.0",
         "links": [
            {
               "href": "https://{Endpoint}/v2.0",
               "rel": "self"
            }
         ]
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.1.2 Pagination

Function

Neutron APIs v2.0 provides the pagination function. You can set parameters **limit** and **marker** in the URL to enable the desired number of items to be returned. All returned items are displayed in the ascending order of ID.

- To access the next page of the request, perform the following configurations:
  - Replace the value of **marker** in the original access request URL. Replace the value of **marker** to the value of **marker** in the value of **href** if the value of **rel** in the response is **next**.
  - Set the value of **page_reverse** to **False**.
- To access the previous page of the request, perform the following configurations:
  - Replace the value of **marker** in the original access request URL. Replace the value of **marker** to the value of **marker** in the value of **href** if the value of **rel** in the response is **previous**.
  - Set the value of **page_reverse** to **True**.

Request Parameters

Table 6-4 Request parameter

Parameter	Type	Mandatory	Description
limit	Integer	No	Specifies the number of items displayed per page.
marker	String	No	Specifies the ID of the last item in the previous list. If the marker value is invalid, error code 400 will be returned.
page_reverse	Boolean	No	Specifies the page direction. The value can be **True** or **False**.

Example Request

- When **page_reverse** is set to **False**:

```
GET https://{Endpoint}/v2.0/networks?limit=2&marker=3d42a0d4-a980-4613-ae76-a2cddecff054&page_reverse=False
```

- When **page_reverse** is set to **True**:

```
GET https://{Endpoint}/v2.0/vpc/peerings?limit=2&marker=e5a0c88e-228e-4e62-a8b0-90825b1b7958&page_reverse=True
```


Response Parameters

Table 6-5 Response parameter

Parameter	Type	Description
{resources}_links	Array of **{resources}_link** objects	Specifies the pagination information. For details, see **Table 6-6**. **{*resources*}** indicates the resource name, for example, **ports**, **networks**, **subnets**, **routers**, **firewall_rules**, **firewall_policies**, **firewall_groups**, **security_groups**, and **security_group_rules**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-6 {resources}_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	The API link is used to query the next or previous page. **next**: The next page is queried. **previous**: The previous page is queried.

Example Response

- When **page_reverse** is set to **False**:

```
{
  "networks": [
    {
      "status": "ACTIVE",
      "subnets": [],
      "name": "liudongtest ",
      "admin_state_up": false,
      "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
      "id": "60c809cb-6731-45d0-ace8-3bf5626421a9"
    },
    {
      "status": "ACTIVE",
      "subnets": [
        "132dc12d-c02a-4c90-9cd5-c31669aace04"
      ],
      "name": "publicnet",
      "admin_state_up": true,
      "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
      "id": "9daeac7c-a98f-430f-8e38-67f9c044e299"
    }
  ],
  "networks_links": [
```

```
    {
        "href": "http://192.168.82.231:9696/v2.0/networks?limit=2&marker=9daeac7c-
a98f-430f-8e38-67f9c044e299",
        "rel": "next"
    },
    {
        "href": "http://192.168.82.231:9696/v2.0/networks?limit=2&marker=60c809cb-6731-45d0-
ace8-3bf5626421a9&page_reverse=True",
        "rel": "previous"
    }
  ]
}
```

- When **page_reverse** is set to **True**:

```
{
  "peerings_links": [
    {
      "marker": "dd442819-5638-401c-bd48-a82703cf0464",
      "rel": "next"
    },
    {
      "marker": "1e13cbaf-3ce4-413d-941f-66d855dbfa7f",
      "rel": "previous"
    }
  ],
  "peerings": [
    {
      "status": "ACTIVE",
      "accept_vpc_info": {
        "vpc_id": "83a48834-b9bc-4f70-aa46-074568594650",
        "tenant_id": "e41a43bf06e249678413c6d61536eff9"
      },
      "request_vpc_info": {
        "vpc_id": "db8e7687-e43b-4fc1-94cf-16f69f484d6d",
        "tenant_id": "e41a43bf06e249678413c6d61536eff9"
      },
      "name": "peering1",
      "id": "1e13cbaf-3ce4-413d-941f-66d855dbfa7f"
    },
    {
      "status": "ACTIVE",
      "accept_vpc_info": {
        "vpc_id": "83a48834-b9bc-4f70-aa46-074568594650",
        "tenant_id": "e41a43bf06e249678413c6d61536eff9"
      },
      "request_vpc_info": {
        "vpc_id": "bd63cc9e-e7b8-4d4e-a0e9-055031470ffc",
        "tenant_id": "e41a43bf06e249678413c6d61536eff9"
      },
      "name": "peering2",
      "id": "dd442819-5638-401c-bd48-a82703cf0464"
    }
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.2 Port

6.2.1 Querying Ports

Function

Queries all networks accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/ports

Example:

```
GET https://{Endpoint}/v2.0/ports?
id={port_id}&name={port_name}&admin_state_up={is_admin_status_up}&network_id={network_id}&mac_address={port_mac}&device_id={port_device_id}&device_owner={device_owner}&tenant_id={tenant_id}&status={port_status}&fixed_ips=ip_address={ip_address}&fixed_ips=subnet_id={subnet_id}
```

Example of querying ports by page

```
GET https://{Endpoint}/v2.0/ports?limit=2&marker=791870bd-36a7-4d9b-b015-a78e9b06af08&page_reverse=False
```

Table 6-7 describes the parameters.

Table 6-7 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies the port ID that is used as the filter.
name	No	String	Specifies the port name that is used as the filter.
admin_state_up	No	Boolean	• Specifies the administrative state of the port that is used as the filter. • The value can be **true** or **false**.
network_id	No	String	Specifies the network ID that is used as the filter. **NOTE** To obtain the network ID: • Method 1: Log in to the VPC console and click the target subnet on the **Subnets** page. You can view the network ID on the displayed page. • Method 2: Call the API for querying subnets. For details, see **Querying Subnets**.
mac_address	No	String	Specifies the MAC address that is used as the filter.

Parameter	Mandatory	Type	Description
device_id	No	String	Specifies the device ID that is used as the filter.
device_owner	No	String	Specifies the device owner that is used as the filter.
status	No	String	• Specifies the status of the port that is used as the filter. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	No	Array of strings	Specifies the ID of the security group that is used as the filter.
fixed_ips	No	Array of strings	Filter by IP address of the port, that is **fixed_ips=ip_address={ip_address}** or **fixed_ips=subnet_id={subnet_id}**. Set *{ip_address}* to an IP address, for example, 192.168.21.22 or 2a07:b980:4030:14::1. Set *{subnet_id}* to the IPv4 or IPv6 subnet ID, for example, 011fc878-5521-4654-a1ad-f5b0b5820302.
tenant_id	No	String	Specifies the project ID that is used as the filter.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Message

None

Example Request

Example 1

```
GET https://{Endpoint}/v2.0/ports?limit=1
```

Example 2

```
GET https://{Endpoint}/v2.0/ports?mac_address=fa:16:3e:f1:0b:09
```


Example 3

```
GET https://{Endpoint}/v2.0/ports?admin_state_up=False
```

Example 4

```
GET https://{Endpoint}/v2.0/ports?device_id=e6c05704-c907-4cc1-8106-69b0996c43b9
```

Example 5

```
GET https://{Endpoint}/v2.0/ports?tenant_id=6c9298ec8c874f7f99688489ab65f90e&name=port_vm_50_3
```

Example 6

```
GET https://{Endpoint}/v2.0/ports?name=port_vm_50_3
```

Response Parameter

Table 6-8 Response parameter

Parameter	Type	Description
ports	Array of **port** objects	Specifies the port object list. For details, see **Table 6-9**.
ports_links	Array of **ports_link** objects	Specifies the pagination information. For details, see **Table 6-15**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-9 port objects

Attribute	Type	Description
id	String	• Specifies the port ID. The value can contain a maximum of 255 characters. • This parameter is not mandatory when you query ports.
name	String	Specifies the port name.
network_id	String	Specifies the ID of the network that the port belongs to.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The default value is **true**.

Attribute	Type	Description
mac_address	String	• Specifies the port MAC address, for example, **"mac_address": "fa:16:3e:9e:ff:55"**. • The MAC address can only be dynamically assigned by the system.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For details, see **Table 6-10**. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. "fixed_ips": [{"subnet_id": "1fd001aa-6946-4168-86d9-924c7d3ef8fb", "ip_address": "2a07:b980:4030:14::1"}]
device_id	String	• Specifies the ID of the device that the port belongs to. • This parameter is automatically maintained by the system and cannot be set or updated manually. The port with this field specified cannot be deleted.

Attribute	Type	Description
device_owner	String	• Specifies the belonged device, which can be the DHCP server, router, or Nova. • The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). • Instructions: – This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**. – The port with this field specified cannot be deleted.
tenant_id	String	Specifies the project ID.
status	String	• Specifies the port status. • The value can be **ACTIVE**, **BUILD**, or **DOWN**. • The status of a HANA SR-IOV VM port is always **DOWN**.

Attribute	Type	Description
security_groups	Array of strings	• Specifies the security group UUID, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. This is an extended attribute. • This parameter cannot be left blank.
allowed_address_pairs	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. This is an extended attribute. For details, see **Table 6-11**. • Instructions: – The IP address cannot be **0.0.0.0**. – Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). – If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. – In the hardware SDN networking plan, the **ip_address** attribute value cannot be in CIDR format. – To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication. – Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.

Attribute	Type	Description
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended DHCP option. This is an extended attribute. For details, see **Table 6-12**.
binding:vif_details	**binding:vif_details** object	For details, see **Table 6-13**.

Attribute	Type	Description
binding:profile	Object	• Specifies the user-defined settings. This is an extended attribute. • Instructions: – The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. The value of this field is maintained by the system and cannot be changed. Example: {"internal_elb": true} – The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect. – For Consumer Cloud, the values of **udp_srvports** and **tcp_srvports** fields are strings. By default, **udp_srvports** and **tcp_srvports** are not

Attribute	Type	Description
		specified. You can set **udp_srvports** and **tcp_srvports** to port numbers, which indicates that the TCP and UDP packets support highly concurrently connections. However, these packets are not protected by network ACLs and security group rules. The **udp_srvports** and **tcp_srvports** fields can be updated concurrently. Format: {"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"} You can enter a maximum of 15 port numbers for each value. Use a space to separate adjacent port numbers. The port number ranges from 1 to 65535. Example: {"tcp_srvports": "80 443", "udp_srvports": "53"} This example indicates that inbound TCP packets to ports 80 and 443, and inbound UDP packets to port 53 support highly concurrent connections. However, these packets are not controlled by network ACL and security group rules.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • The value can be: – **normal** indicates software switching.

Attribute	Type	Description
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. **true** indicates that security groups can be added and DHCP anti-spoofing is enabled. **false** indicates that security groups and DHCP anti-spoofing are not applied.
dns_assignment	Array of **dns_assignment** objects	• Specifies the default private domain name information of the primary NIC. This is an extended attribute. • This parameter is automatically maintained by the system and cannot be set or updated manually. • The value can be: – **hostname**: The same as the value specified for **dns_name**. – **ip_address**: Private IPv4 address of the port. – **fqdn**: Private network fully qualified domain name (FQDN) of the port.
dns_name	String	• Specifies the default private network DNS name of the primary NIC. This is an extended attribute. • This parameter is automatically maintained by the system and cannot be set or updated manually. Before accessing the default private network domain name, ensure that the subnet uses the DNS provided by the current system.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Attribute	Type	Description
created_at	String	• Specifies the time (UTC) when the port is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the port is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-10 fixed_ip objects

Attribute	Type	Description
subnet_id	String	• Specifies the subnet ID. • This parameter cannot be updated.
ip_address	String	• Specifies the port IP address. • This parameter cannot be updated.

Table 6-11 allowed_address_pairs objects

Parameter	Mandatory	Type	Description
ip_address	Yes	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of parameter **allowed_address_pairs** is specified, parameter **ip_address** is mandatory.

Parameter	Mandatory	Type	Description
mac_address	No	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 6-12 extra_dhcp_opt objects

Attribute	Type	Description
opt_name	String	Specifies the option name.
opt_value	String	Specifies the option value.

Table 6-13 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Table 6-14 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Table 6-15 ports_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

Example 1

```
{
 "ports": [{
      "id": "791870bd-36a7-4d9b-b015-a78e9b06af08",
      "name": "port-test",
      "status": "DOWN",
      "admin_state_up": true,
      "fixed_ips": [],
      "mac_address": "fa:16:3e:01:e0:b2",
      "network_id": "00ae08c5-f727-49ab-ad4b-b069398aa171",
      "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
      "project_id": "db82c9e1415a464ea68048baa8acc6b8",
      "device_id": "",
      "device_owner": "",
      "security_groups": ["d0d58aa9-cda9-414c-9c52-6c3daf8534e6"],
      "extra_dhcp_opts": [],
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "binding:vif_details": {},
      "binding:profile": {},
      "port_security_enabled": true,
      "created_at": "2018-09-13T01:43:41",
      "updated_at": "2018-09-13T01:43:41"
 },
{
   "id": "7a8c720d-32b7-47cc-a943-23e48d69e30a",
   "name": "a8d001aa-6946-4168-86d9-924c7d3ef8fb",
   "status": "DOWN",
   "admin_state_up": true,
   "fixed_ips": [
      {
         "subnet_id": "a8d001aa-6946-4168-86d9-924c7d3ef8fb",
         "ip_address": "2a07:b980:4030:14::1"
      }
   ],
   "mac_address": "fa:16:3e:57:39:c3",
   "network_id": "26cf88ff-1a8c-4233-a8e6-183e1e299357",
   "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
   "project_id": "db82c9e1415a464ea68048baa8acc6b8",
   "device_id": "6c2fcea1-b785-4253-b84e-3d887e1c67e1",
   "device_owner": "network:router_interface_distributed",
   "security_groups": ["34acbeed-8f65-4875-86ca-66417b1733fd"],
   "extra_dhcp_opts": [],
   "allowed_address_pairs": [],
   "binding:vnic_type": "normal",
   "binding:vif_details": {},
   "binding:profile": {},
   "port_security_enabled": true,
      "created_at": "2018-09-13T01:43:41",
      "updated_at": "2018-09-13T01:43:41"
}
],
   "ports_links": [
```



```
    {
        "rel": "next",
        "href": "https://{Endpoint}/v2.0/ports?limit=1&marker=7a8c720d-32b7-47cc-a943-23e48d69e30a"
     },
    {   "rel": "previous",
        "href": "https://{Endpoint}/v2.0/ports?limit=1&marker=7a8c720d-32b7-47cc-
a943-23e48d69e30a&page_reverse=True"
     }
  ]
}
```

Example 2

```
{
  "ports": [
    {
      "admin_state_up": true,
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "device_id": "e6c05704-c907-4cc1-8106-69b0996c43b9",
      "device_owner": "compute:az3.dc1",
      "port_security_enabled":true,
      "extra_dhcp_opts": [],
      "fixed_ips": [
        {
          "ip_address": "172.16.0.37",
          "subnet_id": "b3ac1347-63f2-4e82-b853-3d86416a0db5"
        }
      ],
      "dns_assignment": [
        {
          "hostname": "ip-172-16-0-37",
          "ip_address": "172.16.0.37",
          "fqdn": "ip-172-16-0-37.xxx.compute.internal."
        }
      ],
      "dns_name": "ip-172-16-0-37",
      "id": "7bb64706-6e46-4f94-a28a-4bc7caaab87d",
      "mac_address": "fa:16:3e:f1:0b:09",
      "name": "port_vm_50_3",
      "network_id": "a54e1b19-ce78-4b7e-b28b-d2d716cdc161",
      "security_groups": [
        "ef69bc60-2f4b-4f97-b95b-e3b68df0c0b2"
      ],
      "status": "ACTIVE",
      "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
      "project_id": "6c9298ec8c874f7f99688489ab65f90e",
      "created_at": "2018-09-13T01:43:41",
      "updated_at": "2018-09-13T01:43:41"
    }
  ],
  "ports_links": [
    {   "rel": "previous",
        "href": "https://{Endpoint}/v2.0/ports?mac_address=fa%3A16%3A3e%3Af1%3A0b
%3A09&marker=7bb64706-6e46-4f94-a28a-4bc7caaab87d&page_reverse=True"
     }
  ]
}
```

Example 3

```
{
  "ports": [

    {
      "admin_state_up": false,
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "device_id": "",
      "device_owner": "",
```



```
        "port_security_enabled":true,
        "extra_dhcp_opts": [],
        "fixed_ips": [
           {
              "ip_address": "10.100.100.62",
              "subnet_id": "9b28f20c-0234-419f-a0b4-4a84f182f64b"
           }
        ],
        "dns_name": "",
        "id": "ffc0bdee-8413-4fa2-bd82-fa8efe5b3a87",
        "mac_address": "fa:16:3e:2b:bc:57",
        "name": "small_net_port",
        "network_id": "b299b151-7a66-4c6f-a313-cdd3b5724296",
        "security_groups": [
           "ef69bc60-2f4b-4f97-b95b-e3b68df0c0b2"
        ],
        "status": "DOWN",
        "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
        "project_id": "6c9298ec8c874f7f99688489ab65f90e",
        "created_at": "2018-09-13T01:43:41",
        "updated_at": "2018-09-13T01:43:41"
     }
  ],
  "ports_links": [
    {    "rel": "previous",
        "href": "https://{Endpoint}/v2.0/ports?admin_state_up=False&marker=ffc0bdee-8413-4fa2-bd82-
fa8efe5b3a87&page_reverse=True"
     }
  ]
}
```

Example 4

```
{
  "ports": [
     {
        "admin_state_up": true,
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "device_id": "e6c05704-c907-4cc1-8106-69b0996c43b9",
        "device_owner": "compute:az3.dc1",
        "port_security_enabled":true,
        "extra_dhcp_opts": [],
        "fixed_ips": [
           {
              "ip_address": "10.1.0.37",
              "subnet_id": "b3ac1347-63f2-4e82-b853-3d86416a0db5"
           }
        ],
        "dns_assignment": [
           {
              "hostname": "ip-10-1-0-37",
              "ip_address": "10.1.0.37",
              "fqdn": "ip-10-1-0-37.xxx.compute.internal."//xxx indicates the region name.
           }
        ],
        "dns_name": "ip-10-1-0-37",
        "id": "7bb64706-6e46-4f94-a28a-4bc7caaab87d",
        "mac_address": "fa:16:3e:f1:0b:09",
        "name": "port_vm_50_3",
        "network_id": "a54e1b19-ce78-4b7e-b28b-d2d716cdc161",
        "security_groups": [
           "ef69bc60-2f4b-4f97-b95b-e3b68df0c0b2"
        ],
        "status": "ACTIVE",
        "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
        "project_id": "6c9298ec8c874f7f99688489ab65f90e" ,
        "created_at": "2018-09-13T01:43:41",
        "updated_at": "2018-09-13T01:43:41"
     }
```



```
  ],
  "ports_links": [
    {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/ports?device_id=77307088-
ae60-49fb-9146-924dcf1d1402&marker=7bb64706-6e46-4f94-a28a-4bc7caaab87d&page_reverse=True"
    }
  ]
}
```

Example 5

```
{
  "ports": [
    {
      "admin_state_up": true,
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "device_id": "e6c05704-c907-4cc1-8106-69b0996c43b9",
      "device_owner": "compute:az3.dc1",
      "port_secuirty_enabled":true,
      "extra_dhcp_opts": [],
      "fixed_ips": [
        {
          "ip_address": "10.1.0.37",
          "subnet_id": "b3ac1347-63f2-4e82-b853-3d86416a0db5"
        }
      ],
      "dns_assignment": [
        {
          "hostname": "ip-10-1-0-37",
          "ip_address": "10.1.0.37",
          "fqdn": "ip-10-1-0-37.xxx.compute.internal."//xxx indicates the region name.
        }
      ],
      "dns_name": "ip-10-1-0-37",
      "id": "7bb64706-6e46-4f94-a28a-4bc7caaab87d",
      "mac_address": "fa:16:3e:f1:0b:09",
      "name": "port_vm_50_3",
      "network_id": "a54e1b19-ce78-4b7e-b28b-d2d716cdc161",
      "security_groups": [
        "ef69bc60-2f4b-4f97-b95b-e3b68df0c0b2"
      ],
      "status": "ACTIVE",
      "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
      "project_id": "6c9298ec8c874f7f99688489ab65f90e" ,
      "created_at": "2018-09-13T01:43:41",
      "updated_at": "2018-09-13T01:43:41"
    }
  ],
  "ports_links": [
    {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/ports?
tenant_id=6c9298ec8c874f7f99688489ab65f90e&name=port_vm_50_3&marker=7bb64706-6e46-4f94-
a28a-4bc7caaab87d&page_reverse=True"
    }
  ]
}
```

Example 6

```
{
  "ports": [
    {
      "status": "DOWN",
      "allowed_address_pairs": [],
      "extra_dhcp_opts": [],
      "device_owner": "",
      "port_security_enabled":true,
      "fixed_ips": [
        {
```



```
                "subnet_id": "391c74f7-e3b1-405c-8473-2f71a0aec7dc",
                "ip_address": "10.1.0.33"
            }
        ],
        "dns_name": "",
        "id": "0f405555-739f-4a19-abb7-ec11d005b3a9",
        "security_groups": [
            "043548bc-1020-4be0-885a-caac8530e8f6"
        ],
        "device_id": "",
        "port_security_enabled":true,
        "name": "port_vm_50_3",
        "admin_state_up": true,
        "network_id": "9898a82d-7795-4ad5-bf2c-0ed8b822be4f",
        "tenant_id": "3e4a1816927f405cacbc3dca1e05111e",
        "project_id": "3e4a1816927f405cacbc3dca1e05111e",
        "created_at": "2018-09-13T01:43:41",
        "updated_at": "2018-09-13T01:43:41",
        "binding:vnic_type": "normal",
        "mac_address": "fa:16:3e:b0:d9:cf"
    },
    {
        "status": "ACTIVE",
        "allowed_address_pairs": [],
        "extra_dhcp_opts": [],
        "device_owner": "compute:az3.dc1",
        "port_security_enabled":true,
        "fixed_ips": [
            {
                "subnet_id": "b3ac1347-63f2-4e82-b853-3d86416a0db5",
                "ip_address": "10.1.0.37"
            }
        ],
        "dns_assignment": [
            {
                "hostname": "ip-10-1-0-37",
                "ip_address": "10.1.0.37",
                "fqdn": "ip-10-1-0-37.xxx.compute.internal."//xxx indicates the region name.
             }
        ],
        "dns_name": "ip-10-1-0-37",
        "id": "7bb64706-6e46-4f94-a28a-4bc7caaab87d",
        "security_groups": [
            "ef69bc60-2f4b-4f97-b95b-e3b68df0c0b2"
        ],
        "device_id": "e6c05704-c907-4cc1-8106-69b0996c43b9",
        "name": "port_vm_50_3",
        "admin_state_up": true,
        "network_id": "a54e1b19-ce78-4b7e-b28b-d2d716cdc161",
        "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
        "project_id": "3e4a1816927f405cacbc3dca1e05111e",
        "created_at": "2018-09-13T01:43:41",
        "updated_at": "2018-09-13T01:43:41",
         "binding:vnic_type": "normal",
        "binding:vnic_type": "normal",
        "mac_address": "fa:16:3e:f1:0b:09"
    }
  ],
  "ports_links": [
    {    "rel": "previous",
        "href": "https://{Endpoint}/v2.0/ports?name=port_vm_50_3&marker=0f405555-739f-4a19-abb7-
ec11d005b3a9&page_reverse=True"
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.2.2 Querying a Port

Function

This API is used to query details about a specified port.

URI

GET /v2.0/ports/{port_id}

Table 6-16 describes the parameters.

Table 6-16 Parameter description

Parameter	Mandatory	Description
port_id	Yes	Specifies the port ID that uniquely identifies the port.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/ports/791870bd-36a7-4d9b-b015-a78e9b06af08
```

Response Parameters

Table 6-17 Response parameter

Parameter	Type	Description
port	**port** object	Specifies the port object list. For details, see **Table 6-18**.

Table 6-18 port objects

Attribute	Type	Description
id	String	• Specifies the port ID. The value can contain a maximum of 255 characters. • This parameter is not mandatory when you query ports.
name	String	Specifies the port name.
network_id	String	Specifies the ID of the network that the port belongs to.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The default value is **true**.
mac_address	String	• Specifies the port MAC address, for example, **"mac_address": "fa:16:3e:9e:ff:55"**. • The MAC address can only be dynamically assigned by the system.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For details, see **Table 6-19**. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. **"fixed_ips": [{"subnet_id": "1fd001aa-6946-4168-86d9-924c7d3ef8fb", "ip_address": "2a07:b980:4030:14::1"}]**.
device_id	String	• Specifies the device ID. • This parameter is automatically maintained by the system and cannot be set or updated manually. The port with this field specified cannot be deleted.

Attribute	Type	Description
device_owner	String	• Specifies the belonged device, which can be the DHCP server, router, or Nova. • The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). • Instructions: – This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**. – The port with this field specified cannot be deleted.
tenant_id	String	Specifies the project ID.
status	String	• Specifies the port status. • The value can be **ACTIVE**, **BUILD**, or **DOWN**. • The status of a HANA SR-IOV VM port is always **DOWN**.

Attribute	Type	Description
security_groups	Array of strings	• Specifies the security group UUID, for example, "security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]. This is an extended attribute. • This parameter cannot be left blank.
allowed_address_pairs	Array of **allowed_address_pairs** objects	• Specifies the IP address and MAC address pair. This is an extended attribute. For details, see **Table 6-20**. • Instructions: – The IP address cannot be **0.0.0.0**. – Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). – If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. – In the hardware SDN networking plan, the **ip_address** attribute value cannot be in CIDR format. – To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication. – Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended DHCP option. This is an extended attribute. For details, see **Table 6-21**.

Attribute	Type	Description
binding:vif_details	**binding:vif_details** object	For details, see **Table 6-23**.

Attribute	Type	Description
binding:profile	binding:profile object	• Specifies the user-defined settings. This is an extended attribute. • Instructions: – The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. The value of this field is maintained by the system and cannot be changed. Example: {"internal_elb": true} – The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect. – For Consumer Cloud, the values of **udp_srvports** and **tcp_srvports** fields are strings. By default, **udp_srvports** and **tcp_srvports** are not

Attribute	Type	Description
		specified. You can set **udp_srvports** and **tcp_srvports** to port numbers, which indicates that the TCP and UDP packets support highly concurrently connections. However, these packets are not protected by network ACLs and security group rules. The **udp_srvports** and **tcp_srvports** fields can be updated concurrently. Format: {"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"} You can enter a maximum of 15 port numbers for each value. Use a space to separate adjacent port numbers. The port number ranges from 1 to 65535. Example: {"tcp_srvports": "80 443", "udp_srvports": "53"} This example indicates that inbound TCP packets to ports 80 and 443, and inbound UDP packets to port 53 support highly concurrent connections. However, these packets are not controlled by network ACL and security group rules.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • The value can be: – **normal** indicates software switching.

Attribute	Type	Description
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. **true** indicates that security groups can be added and DHCP anti-spoofing is enabled. **false** indicates that security groups and DHCP anti-spoofing are not applied.
dns_assignment	Array of **dns_assignment** objects	• Specifies the default private domain name information of the primary NIC. This is an extended attribute. • This parameter is automatically maintained by the system and cannot be set or updated manually. • The value can be: – **hostname**: The same as the value specified for **dns_name**. – **ip_address**: Private IPv4 address of the port. – **fqdn**: Private network fully qualified domain name (FQDN) of the port.
dns_name	String	• Specifies the default private network DNS name of the primary NIC. This is an extended attribute. • This parameter is automatically maintained by the system and cannot be set or updated manually. Before accessing the default private network domain name, ensure that the subnet uses the DNS provided by the current system.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Attribute	Type	Description
created_at	String	• Specifies the time (UTC) when the port is created. • Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	• Specifies the time (UTC) when the port is updated. • Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-19 fixed_ip objects

Attribute	Type	Description
subnet_id	String	• Specifies the subnet ID. • This parameter cannot be updated.
ip_address	String	• Specifies the port IP address. • This parameter cannot be updated.

Table 6-20 allowed_address_pairs objects

Parameter	Mandatory	Type	Description
ip_address	Yes	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of parameter **allowed_address_pairs** is specified, parameter **ip_address** is mandatory.

Parameter	Mandatory	Type	Description
mac_address	No	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 6-21 extra_dhcp_opt objects

Attribute	Type	Description
opt_name	String	Specifies the option name.
opt_value	String	Specifies the option value.

Table 6-22 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Table 6-23 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Example Response

```
{
    "port": {
```



```
    "id": "791870bd-36a7-4d9b-b015-a78e9b06af08",
    "name": "port-test",
    "status": "DOWN",
    "admin_state_up": true,
    "fixed_ips": [],
    "mac_address": "fa:16:3e:01:e0:b2",
    "network_id": "00ae08c5-f727-49ab-ad4b-b069398aa171",
    "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
    "project_id": "db82c9e1415a464ea68048baa8acc6b8",
    "device_id": "",
    "device_owner": "",
    "security_groups": [
        "d0d58aa9-cda9-414c-9c52-6c3daf8534e6"
    ],
    "extra_dhcp_opts": [],
    "allowed_address_pairs": [],
    "binding:vnic_type": "normal",
    "binding:vif_details": {},
    "binding:profile": {},
    "port_security_enabled": true,
    "created_at": "2018-09-13T01:43:41",
    "updated_at": "2018-09-13T01:43:41"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.2.3 Creating a Port

Function

This API is used to create a port.

URI

POST /v2.0/ports

Request Parameters

Table 6-24 Request parameter

Parameter	Type	Mandatory	Description
port	**port** object	Yes	Specifies the port object list. For details, see **Table 6-25**.

Table 6-25 port objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the port name.
network_id	Yes	String	• Specifies the ID of the network to which the port belongs. • The network ID must exist. **NOTE** To obtain the network ID: • Method 1: Log in to the VPC console and click the target subnet on the **Subnets** page. You can view the network ID on the displayed page. • Method 2: Call the API for querying subnets. For details, see **Querying Subnets**.
admin_state_up	No	Boolean	Specifies the administrative status. The default value is **true**.
fixed_ips	No	Array of **fixed_ip** objects	Specifies the port IP address. For details, see **Table 6-26**. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. "fixed_ips": [{"subnet_id": "1fd001aa-6946-4168-86d9-924c7d3ef8fb", "ip_address": "2a07:b980:4030:14::1"}]
security_groups	No	Array of strings	Specifies the UUID of the security group, for example, **"security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]**. This is an extended attribute. This parameter cannot be left blank.

Attribute	Mandatory	Type	Description
allowed_address_pairs	No	Array of **allowed_address_pairs** objects	Specifies the IP address and MAC address pair. This is an extended attribute. For details, see **Table 6-27**. Instructions: • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • In the hardware SDN networking plan, the **ip_address** attribute value cannot be in CIDR format. • To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the extended DHCP option. This is an extended attribute. For details, see **Table 6-28**.

Attribute	Mandatory	Type	Description
binding:profile	No	Object	• Specifies the user-defined settings. This is an extended attribute. • Instructions: – The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. The value of this field is maintained by the system and cannot be changed. Example: {"internal_elb": true} – The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect. – For Consumer Cloud, the values of

Attribute	Mandatory	Type	Description
			udp_srvports and **tcp_srvports** fields are strings. By default, **udp_srvports** and **tcp_srvports** are not specified. You can set **udp_srvports** and **tcp_srvports** to port numbers, which indicates that the TCP and UDP packets support highly concurrently connections. However, these packets are not protected by network ACLs and security group rules. The **udp_srvports** and **tcp_srvports** fields can be updated concurrently. Format: {"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"} You can enter a maximum of 15 port numbers for each value. Use a space to separate adjacent port numbers. The port number ranges from 1 to 65535. Example: {"tcp_srvports": "80 443", "udp_srvports": "53"} This example indicates that inbound TCP packets to ports 80 and 443, and inbound UDP packets to port 53 support highly concurrent connections. However, these packets are not controlled by network ACL and security group rules.

Attribute	Mandatory	Type	Description
binding:vnic_type	No	String	Specifies the type of the bound vNIC. **normal**: Softswitch
port_security_enabled	No	Boolean	Specifies whether the security option is enabled for the port. **true** indicates that security groups can be added and DHCP anti-spoofing is enabled. **false** indicates that security groups and DHCP anti-spoofing are not applied.
device_owner	No	String	Specifies the device that the port belongs to. Currently, only **""** and **neutron:VIP_PORT** are supported. **neutron:VIP_PORT** indicates the port of a virtual IP address.

Table 6-26 fixed_ip objects

Attribute	Mandatory	Type	Description
subnet_id	No	String	Specifies the ID of the subnet to which the port belongs. This parameter cannot be updated.
ip_address	No	String	Specifies the port IP address. This parameter cannot be updated.

Table 6-27 allowed_address_pairs objects

Parameter	Mandatory	Type	Description
ip_address	Yes	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of parameter **allowed_address_pairs** is specified, parameter **ip_address** is mandatory.
mac_address	No	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 6-28 extra_dhcp_opt objects

Attribute	Mandatory	Type	Description
opt_name	No	String	Specifies the option name.
opt_value	No	String	Specifies the option value.

Example Request

Create a port named **port-test** on network whose ID is 00ae08c5-f727-49ab-ad4b-b069398aa171.

```
POST https://{Endpoint}/v2.0/ports

{
    "port": {
        "admin_state_up": true,
        "network_id": "00ae08c5-f727-49ab-ad4b-b069398aa171",
        "name": "port-test"
    }
}
```


Response Parameters

Table 6-29 Response parameter

Parameter	Type	Description
port	**port** object	Specifies the port information. For details, see **Table 6-30**.

Table 6-30 port objects

Attribute	Type	Description
id	String	Specifies the port ID. A maximum of 255 characters are allowed. This parameter is not mandatory when you query ports.
name	String	Specifies the port name.
network_id	String	Specifies the ID of the network to which the port belongs.
admin_state_up	Boolean	Specifies the administrative status. The default value is **true**.
mac_address	String	Specifies the port MAC address. For example, **"mac_address": "fa:16:3e:9e:ff:55"**. This value can only be dynamically assigned by the system.
fixed_ips	Array of **fixed_ip** objects	Specifies the port IP address. For details, see **Table 6-31**. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. "fixed_ips": [{"subnet_id": "1fd001aa-6946-4168-86d9-924c7d3ef8fb", "ip_address": "2a07:b980:4030:14::1"}]

Attribute	Type	Description
device_id	String	Specifies the device ID. This value is automatically maintained by the system and cannot be set or updated manually. The port with this field specified cannot be deleted.
device_owner	String	Specifies the DHCP, router or Nova to which a device belongs. The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter of a port is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**. The port with this field specified cannot be deleted.
tenant_id	String	Specifies the project ID.
status	String	Specifies the port status. The value can be **ACTIVE**, **BUILD**, or **DOWN**. The status of a HANA SR-IOV VM port is always **DOWN**.

Attribute	Type	Description
security_groups	Array of strings	Specifies the UUID of the security group, for example, **"security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]**. This is an extended attribute. This parameter cannot be left blank.
allowed_address_pairs	Array of **allowed_address_pairs** objects	Specifies the IP address and MAC address pair. This is an extended attribute. For details, see **Table 6-32**. Instructions: • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • In the hardware SDN networking plan, the **ip_address** attribute value cannot be in CIDR format. • To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended DHCP option. This is an extended attribute. For details, see **Table 6-33**.
binding:vif_details	**binding:vif_details** object	For details, see **Table 6-34**.

Attribute	Type	Description
binding:profile	Object	• Specifies the user-defined settings. This is an extended attribute. • Instructions: – The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. The value of this field is maintained by the system and cannot be changed. Example: {"internal_elb": true} – The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect. – For Consumer Cloud, the values of **udp_srvports** and **tcp_srvports** fields are strings. By default, **udp_srvports** and **tcp_srvports** are not

Attribute	Type	Description
		specified. You can set **udp_srvports** and **tcp_srvports** to port numbers, which indicates that the TCP and UDP packets support highly concurrently connections. However, these packets are not protected by network ACLs and security group rules. The **udp_srvports** and **tcp_srvports** fields can be updated concurrently. Format: {"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"} You can enter a maximum of 15 port numbers for each value. Use a space to separate adjacent port numbers. The port number ranges from 1 to 65535. Example: {"tcp_srvports": "80 443", "udp_srvports": "53"} This example indicates that inbound TCP packets to ports 80 and 443, and inbound UDP packets to port 53 support highly concurrent connections. However, these packets are not controlled by network ACL and security group rules.
binding:vnic_type	String	Specifies the type of the bound vNIC. **normal**: Softswitch
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect.

Attribute	Type	Description
dns_assignment	Array of **dns_assignment** objects	Specifies the default private network domain name information of the primary NIC. This is an extended attribute. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value. • **hostname**: **dns_name** value of the NIC • **ip_address**: Private IPv4 address of the NIC • **fqdn**: Default private network fully qualified domain name (FQDN) of the IP address
dns_name	String	Specifies the default private network DNS name of the primary NIC. This is an extended attribute. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value. Before accessing the default private network domain name, ensure that the subnet uses the DNS provided by the current system.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the port is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the port is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-31 fixed_ip objects

Attribute	Type	Description
subnet_id	String	Specifies the ID of the subnet to which the port belongs. This parameter cannot be updated.
ip_address	String	Specifies the port IP address. This parameter cannot be updated.

Table 6-32 allowed_address_pairs objects

Attribute	Type	Description
ip_address	String	Specifies the IP address. This parameter cannot be **0.0.0.0**.
mac_address	String	Specifies the MAC address.

Table 6-33 extra_dhcp_opt objects

Attribute	Type	Description
opt_name	String	Specifies the option name.
opt_value	String	Specifies the option value.

Table 6-34 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Table 6-35 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.

Parameter	Type	Description
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Example Response

```
{
    "port": {
        "id": "a7d98f3c-b42f-460b-96a1-07601e145961",
        "name": "port-test",
        "status": "DOWN",
        "admin_state_up": true,
        "fixed_ips": [],
        "mac_address": "fa:16:3e:01:f7:90",
        "network_id": "00ae08c5-f727-49ab-ad4b-b069398aa171",
        "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
        "project_id": "db82c9e1415a464ea68048baa8acc6b8",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "d0d58aa9-cda9-414c-9c52-6c3daf8534e6"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "binding:vif_details": {},
        "binding:profile": {},
        "port_security_enabled": true,
        "created_at": "2018-09-20T01:45:26",
        "updated_at": "2018-09-20T01:45:26"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.2.4 Updating a Port

Function

This API is used to update a port.

URI

PUT /v2.0/ports/{port_id}

Table 6-36 describes the parameters.

Table 6-36 Parameter description

Parameter	Mandatory	Description
port_id	Yes	Specifies the port ID that uniquely identifies the port.

Request Parameters

Table 6-37 Request parameter

Parameter	Type	Mandatory	Description
port	**port** object	Yes	Specifies the port object list. For details, see **Table 6-38**. You must specify at least one attribute when updating a port.

Table 6-38 port objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the port name.
security_groups	No	Array of strings	Specifies the UUID of the security group, for example, **"security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]**. This is an extended attribute. This parameter cannot be left blank.

Attribute	Mandatory	Type	Description
allowed_address_pairs	No	Array of **allowed_address_pairs** objects	Specifies the IP address and MAC address pair. This is an extended attribute. For details, see **Table 6-39**. Instructions: • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • In the hardware SDN networking plan, the **ip_address** attribute value cannot be in CIDR format. • To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the extended DHCP option. This is an extended attribute. For details, see **Table 6-40**.

Attribute	Mandatory	Type	Description
binding:profile	No	Object	• Specifies the user-defined settings. This is an extended attribute. • Instructions: – The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. The value of this field is maintained by the system and cannot be changed. Example: {"internal_elb": true} – The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.

Attribute	Mandatory	Type	Description
			– For Consumer Cloud, the values of **udp_srvports** and **tcp_srvports** fields are strings. By default, **udp_srvports** and **tcp_srvports** are not specified. You can set **udp_srvports** and **tcp_srvports** to port numbers, which indicates that the TCP and UDP packets support highly concurrently connections. However, these packets are not protected by network ACLs and security group rules. The **udp_srvports** and **tcp_srvports** fields can be updated concurrently. Format: {"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"} You can enter a maximum of 15 port numbers for each value. Use a space to separate adjacent port numbers. The port number ranges from 1 to 65535. Example: {"tcp_srvports": "80 443", "udp_srvports": "53"} This example indicates that inbound TCP packets to ports 80 and 443, and inbound UDP packets to port 53 support highly concurrent connections. However, these packets

Attribute	Mandatory	Type	Description
			are not controlled by network ACL and security group rules.
binding:vnic_type	No	String	Specifies the type of the bound vNIC. **normal**: Softswitch
port_security_enabled	No	Boolean	Specifies whether the security option is enabled for the port. **true** indicates that security groups can be added and DHCP anti-spoofing is enabled. **false** indicates that security groups and DHCP anti-spoofing are not applied.

Table 6-39 allowed_address_pairs objects

Parameter	Mandatory	Type	Description
ip_address	Yes	String	• Specifies the IP address. • You cannot set it to **0.0.0.0/0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**. • If the value of parameter **allowed_address_pairs** is specified, parameter **ip_address** is mandatory.
mac_address	No	String	Specifies the MAC address. By default, the MAC address of the local port is used.

Table 6-40 extra_dhcp_opt objects

Attribute	Mandatory	Type	Description
opt_name	No	String	Specifies the option name.
opt_value	No	String	Specifies the option value.

Example Request

Change the name of the port whose ID is 7a9a954a-eb41-4954-a300-11ab17a361a2 to **port-test02**.

```
PUT https://{Endpoint}/v2.0/ports/7a9a954a-eb41-4954-a300-11ab17a361a2

{
   "port": {
        "name": "port-test02"
   }
}
```

Response Parameters

Table 6-41 Response parameter

Parameter	Type	Description
port	**port** object	Specifies the port object list. For details, see **Table 6-42**.

Table 6-42 port objects

Attribute	Type	Description
id	String	Specifies the port ID. A maximum of 255 characters are allowed. This parameter is not mandatory when you query ports.
name	String	Specifies the port name.
network_id	String	Specifies the ID of the network to which the port belongs.
admin_state_up	Boolean	Specifies the administrative status. The default value is **true**.

Attribute	Type	Description
mac_address	String	Specifies the port MAC address. For example, **"mac_address": "fa:16:3e:9e:ff:55"**. This value can only be dynamically assigned by the system.
fixed_ips	Array of **fixed_ip** objects	Specifies the port IP address. For details, see **Table 6-43**. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. "fixed_ips": [{"subnet_id": "1fd001aa-6946-4168-86d9-924c7d3ef8fb", "ip_address": "2a07:b980:4030:14::1"}]
device_id	String	Specifies the device ID. This value is automatically maintained by the system and cannot be set or updated manually. The port with this field specified cannot be deleted.

Attribute	Type	Description
device_owner	String	Specifies the DHCP, router or Nova to which a device belongs. The value can be **network:dhcp**, **network:router_interface_distributed**, **compute:xxx**, **neutron:VIP_PORT**, **neutron:LOADBALANCERV2**, **neutron:LOADBALANCERV3**, **network:endpoint_interface**, **network:nat_gateway**, or **network:ucmp**. (In value **compute:xxx**, **xxx** specifies the AZ name, for example, **compute:aa-bb-cc** indicates that the private IP address is used by an ECS in the **aa-bb-cc** AZ). This parameter value cannot be updated. You can only set **device_owner** to **neutron:VIP_PORT** for a virtual IP address port during port creation. If this parameter of a port is not left blank, the port can only be deleted when this parameter value is **neutron:VIP_PORT**. The port with this field specified cannot be deleted.
tenant_id	String	Specifies the project ID.
status	String	Specifies the port status. The value can be **ACTIVE**, **BUILD**, or **DOWN**. The status of a HANA SR-IOV VM port is always **DOWN**.
security_groups	Array of strings	Specifies the UUID of the security group, for example, **"security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]**. This is an extended attribute. This parameter cannot be left blank.

Attribute	Type	Description
allowed_address_pairs	Array of **allowed_address_pairs** objects	Specifies the IP address and MAC address pair. This is an extended attribute. For details, see **Table 6-44**. Instructions: • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. • In the hardware SDN networking plan, the **ip_address** attribute value cannot be in CIDR format. • To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication. • Set **allowed_address_pairs** of the cloud server to **1.1.1.1/0**.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended DHCP option. This is an extended attribute. For details, see **Table 6-45**.
binding:vif_details	**binding:vif_details** object	For details, see **Table 6-46**.

Attribute	Type	Description
binding:profile	Object	• Specifies the user-defined settings. This is an extended attribute. • Instructions: – The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. The value of this field is maintained by the system and cannot be changed. Example: {"internal_elb": true} – The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true } Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect. – For Consumer Cloud, the values of **udp_srvports** and **tcp_srvports** fields are strings. By default, **udp_srvports** and **tcp_srvports** are not

Attribute	Type	Description
		specified. You can set **udp_srvports** and **tcp_srvports** to port numbers, which indicates that the TCP and UDP packets support highly concurrently connections. However, these packets are not protected by network ACLs and security group rules. The **udp_srvports** and **tcp_srvports** fields can be updated concurrently. Format: {"tcp_srvports": "port1 port2 port3", "udp_srvports": "port1 port2 port3"} You can enter a maximum of 15 port numbers for each value. Use a space to separate adjacent port numbers. The port number ranges from 1 to 65535. Example: {"tcp_srvports": "80 443", "udp_srvports": "53"} This example indicates that inbound TCP packets to ports 80 and 443, and inbound UDP packets to port 53 support highly concurrent connections. However, these packets are not controlled by network ACL and security group rules.
binding:vnic_type	String	Specifies the type of the bound vNIC. **normal**: Softswitch
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect.

Attribute	Type	Description
dns_assignment	Array of **dns_assignment** objects	Specifies the default private network domain name information of the primary NIC. This is an extended attribute. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value. • **hostname**: **dns_name** value of the NIC • **ip_address**: Private IPv4 address of the NIC • **fqdn**: Default private network fully qualified domain name (FQDN) of the IP address
dns_name	String	Specifies the default private network DNS name of the primary NIC. This is an extended attribute. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value. Before accessing the default private network domain name, ensure that the subnet uses the DNS provided by the current system.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the port is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the port is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-43 fixed_ip objects

Attribute	Type	Description
subnet_id	String	Specifies the ID of the subnet to which the port belongs. This parameter cannot be updated.
ip_address	String	Specifies the port IP address. This parameter cannot be updated.

Table 6-44 allowed_address_pairs objects

Attribute	Type	Description
ip_address	String	Specifies the IP address. This parameter cannot be **0.0.0.0**.
mac_address	String	Specifies the MAC address.

Table 6-45 extra_dhcp_opt objects

Attribute	Type	Description
opt_name	String	Specifies the option name.
opt_value	String	Specifies the option value.

Table 6-46 binding:vif_details object

Parameter	Type	Description
primary_interface	Boolean	If the value is true, this is the primary NIC.
port_filter	Boolean	Specifies the port used for filtering in security groups to protect against MAC or IP spoofing.
ovs_hybrid_plug	Boolean	Specifies that OVS hybrid plug should be used by Nova APIs.

Table 6-47 dns_assignment object

Parameter	Type	Description
hostname	String	Specifies the host name of the port.

Parameter	Type	Description
ip_address	String	Specifies the port IP address.
fqdn	String	Specifies the private network fully qualified domain name (FQDN) of the port.

Example Response

```
{
    "port": {
        "id": "a7d98f3c-b42f-460b-96a1-07601e145961",
        "name": "port-test02",
        "status": "DOWN",
        "admin_state_up": true,
        "fixed_ips": [],
        "mac_address": "fa:16:3e:01:f7:90",
        "network_id": "00ae08c5-f727-49ab-ad4b-b069398aa171",
        "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
        "project_id": "db82c9e1415a464ea68048baa8acc6b8",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "d0d58aa9-cda9-414c-9c52-6c3daf8534e6"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "binding:vif_details": {},
        "binding:profile": {},
        "port_security_enabled": true,
        "created_at": "2018-09-20T01:45:26",
        "updated_at": "2018-09-20T01:48:56"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.2.5 Deleting a Port

Function

This API is used to delete a port.

Restrictions

- A port with **device_owner** set to a value other than **neutron:VIP_PORT** cannot be deleted.

- A port with **device_id** specified cannot be deleted.

URI

DELETE /v2.0/ports/{port_id}

Table 6-48 describes the parameters.

Table 6-48 Parameter description

Parameter	Mandatory	Description
port_id	Yes	Specifies the port ID that uniquely identifies the port.

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/ports/2b098395-046a-4071-b009-312bcee665cb
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.3 Network

6.3.1 Querying Networks

Function

This API is used to query all networks accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/networks

Example:

```
GET https://{Endpoint}/v2.0/networks?
id={network_id}&status={network_status}&name={network_name}&admin_state_up=$
{admin_state_up}&tenant_id={tenant_id}&shared={is_shared}&provider:network_type={geneve}
```

Example of querying ports by page

```
GET https://{Endpoint}/v2.0/networks?limit=2&marker=0133cd73-34d4-4d4c-bf1f-
e65b24603206&page_reverse=False
```

Table 6-49 describes the parameters.

Table 6-49 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the network ID is used as the filtering condition.
name	No	String	Specifies that the network name is used as the filtering condition.
admin_state_up	No	Boolean	Specifies that the admin state is used as the filtering condition. The value can be **true** or **false**.
provider:network_type	No	String	Specifies that the network type is used as the filtering condition.
shared	No	Boolean	Specifies that whether the network can be shared by multiple tenants is used as the filtering condition. The value can be **true** or **false**.
status	No	String	Specifies that the network status is used as the filtering condition. The value can be **ACTIVE**, **BUILD**, or **DOWN**.
router:external	No	Boolean	Specifies whether the network is an external network is used as the filtering condition. The value can be **true** or **false**.
tenant_id	No	String	Specifies that the project ID is used as the filtering condition.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/networks?limit=1
```


Response Parameters

Table 6-50 Response parameter

Parameter	Type	Description
networks	Array of **network** objects	Specifies the network list. For details, see **Table 6-51**.
networks_links	Array of **networks_link** objects	Specifies the pagination information. For details, see **Table 6-52**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-51 network object

Attribute	Type	Description
status	String	Specifies the network status. The value can be **ACTIVE**, **BUILD**, **DOWN**, or **ERROR**.
subnets	Array of strings	Specifies ID of the subnet associated with this network. Only one subnet can be associated with each network.
name	String	Specifies the network name. The name cannot be the same as the **admin_external_net** value (preset network name and cannot be used).
router:external	Boolean	Specifies whether the network is an external network. The default value is **false**. This is an extended attribute.
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.
tenant_id	String	Specifies the project ID.
shared	Boolean	Specifies whether the network can be shared by different tenants.
id	String	Specifies the network ID.

Attribute	Type	Description
provider:network_type	String	Specifies the network type. Only the VXLAN and GENEVE networks are supported. Tenants can only set this parameter to **geneve**. If this parameter is not specified, the network type is automatically set to VXLAN. If the network is preset as **admin_external_net**, this parameter is fixed at **vlan** and cannot be configured. Note: • Set this parameter to **geneve** if you want to create GENEVE networks. • Do not specify this parameter if you want to create VXLAN networks.
availability_zone_hints	Array of strings	Specifies the availability zones available to this network. The current version does not support cross-availability-zone network scheduling.
availability_zones	Array of strings	Specifies the availability zone of this network.
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping settings of all VMs in the network do not take effect.
dns_domain	String	Specifies the default private network DNS domain address. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the network is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the network is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-52 networks_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

```
{
   "networks": [
      {
         "id": "0133cd73-34d4-4d4c-bf1f-e65b24603206",
         "name": "3804f26c-7862-43b6-ad3c-48445f42de89",
         "status": "ACTIVE",
         "shared": false,
         "subnets": [
            "423796f5-e02f-476f-bf02-2b88c8ddac8b"
         ],
         "availability_zone_hints": [],
         "availability_zones": [
            "az2.dc2",
            "az5.dc5"
         ],
         "admin_state_up": true,
         "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "provider:network_type": "vxlan",
         "router:external": false,
         "port_security_enabled": true,
         "created_at": "2018-03-23T03:51:58",
         "updated_at": "2018-03-23T03:51:58"
      }
   ],
   "networks_links": [
      {
         "rel": "next",
         "href": "https://{Endpoint}/v2.0/networks?limit=1&marker=0133cd73-34d4-4d4c-bf1f-
e65b24603206"
      },
      {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/subnets?limit=1&marker=0133cd73-34d4-4d4c-bf1f-
e65b24603206&page_reverse=True"
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.3.2 Querying Network Details

Function

This API is used to query details about a network.

URI

GET /v2.0/networks/{network_id}

Table 6-53 describes the parameters.

Table 6-53 Parameter description

Parameter	Mandatory	Description
network_id	Yes	Specifies the network ID.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/networks/0133cd73-34d4-4d4c-bf1f-e65b24603206
```

Response Parameters

Table 6-54 Response parameter

Parameter	Type	Description
network	**network** object	Specifies the network. For details, see **Table 6-55**.

Table 6-55 network objects

Attribute	Type	Description
status	String	Specifies the network status. The value can be **ACTIVE**, **BUILD**, **DOWN**, or **ERROR**.
subnets	Array of strings	Specifies IDs of the subnets associated with this network. The IDs are in a list. Only one subnet can be associated with each network.

Attribute	Type	Description
name	String	Specifies the network name. The name cannot be the same as the **admin_external_net** value (preset network name and cannot be used).
router:external	Boolean	Specifies whether the network is an external network. The default value is **false**. This is an extended attribute.
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.
tenant_id	String	Specifies the project ID.
shared	Boolean	Specifies whether the network can be shared by different tenants.
id	String	Specifies the network ID. This parameter is not mandatory when you query networks.
provider:network_type	String	Specifies the network type. Only the VXLAN and GENEVE networks are supported. Tenants can only set this parameter to **geneve**. If this parameter is not specified, the network type is automatically set to VXLAN. If the network is preset as **admin_external_net**, this parameter is fixed at **vlan** and cannot be configured. Note: • Set this parameter to **geneve** if you want to create GENEVE networks. • Do not specify this parameter if you want to create VXLAN networks.
availability_zone_hints	Array of strings	Specifies the availability zones available to this network. The current version does not support cross-availability-zone network scheduling.
availability_zones	Array of strings	Specifies the availability zone of this network.
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping settings of all VMs in the network do not take effect.

Attribute	Type	Description
dns_domain	String	Specifies the default private network DNS domain address. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the network is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the network is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "network": {
        "id": "0133cd73-34d4-4d4c-bf1f-e65b24603206",
        "name": "3804f26c-7862-43b6-ad3c-48445f42de89",
        "status": "ACTIVE",
        "shared": false,
        "subnets": [
            "423796f5-e02f-476f-bf02-2b88c8ddac8b"
        ],
        "availability_zone_hints": [],
        "availability_zones": [
            "az2.dc2",
            "az5.dc5"
        ],
        "admin_state_up": true,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "provider:network_type": "vxlan",
        "router:external": false,
        "port_security_enabled": true,
        "created_at": "2018-03-23T03:51:58",
        "updated_at": "2018-03-23T03:51:58"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.3.3 Creating a Network

Function

This API is used to create a network.

URI

POST /v2.0/networks

Request Parameters

Table 6-56 Request parameter

Parameter	Type	Mandatory	Description
network	**network** object	Yes	Specifies the network. For details, see **Table 6-57**.

Table 6-57 network objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the network name. The name cannot be the same as the **admin_external_net** value (preset network name and cannot be used).
admin_state_up	No	Boolean	Specifies the administrative status. The value can only be **true**.
shared	No	Boolean	Specifies whether the network can be shared by different tenants.

Attribute	Mandatory	Type	Description
provider:network_type	No	String	Specifies the network type. Only the VXLAN and GENEVE networks are supported. Tenants can only set this parameter to **geneve**. If this parameter is not specified, the network type is automatically set to VXLAN. If the network is preset as **admin_external_net**, this parameter is fixed at **vlan** and cannot be configured. Note: • Set this parameter to **geneve** if you want to create GENEVE networks. • Do not specify this parameter if you want to create VXLAN networks.
port_security_enabled	No	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping settings of all VMs in the network do not take effect.

Example Request

Create a network named **network-test**.

```
POST https://{Endpoint}/v2.0/networks

{
    "network": {
        "name": "network-test",
        "shared": false,
        "admin_state_up": true
    }
}
```

Response Parameters

Table 6-58 Response parameter

Parameter	Type	Description
network	**network** object	Specifies the network. For details, see **Table 6-59**.

Table 6-59 network objects

Attribute	Type	Description
status	String	Specifies the network status. The value can be **ACTIVE**, **BUILD**, **DOWN**, or **ERROR**.
subnets	Array of strings	Specifies IDs of the subnets associated with this network. The IDs are in a list. Only one subnet can be associated with each network.
name	String	Specifies the network name. The name cannot be the same as the **admin_external_net** value (preset network name and cannot be used).
router:external	Boolean	Specifies whether the network is an external network. The default value is **false**. This is an extended attribute.
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.
tenant_id	String	Specifies the project ID.
shared	Boolean	Specifies whether the network can be shared by different tenants.
id	String	Specifies the network ID. This parameter is not mandatory when you query networks.
provider:network_type	String	Specifies the network type. Only the VXLAN and GENEVE networks are supported. Tenants can only set this parameter to **geneve**. If this parameter is not specified, the network type is automatically set to VXLAN. If the network is preset as **admin_external_net**, this parameter is fixed at **vlan** and cannot be configured. Note: • Set this parameter to **geneve** if you want to create GENEVE networks. • Do not specify this parameter if you want to create VXLAN networks.

Attribute	Type	Description
availability_zone_hints	Array of strings	Specifies the availability zones available to this network. The current version does not support cross-availability-zone network scheduling.
availability_zones	Array of strings	Specifies the availability zone of this network.
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping settings of all VMs in the network do not take effect.
dns_domain	String	Specifies the default private network DNS domain address. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the network is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the network is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
   "network": {
      "id": "c360322d-5315-45d7-b7d2-481f98c56edb",
      "name": "network-test",
      "status": "ACTIVE",
      "shared": false,
      "subnets": [],
      "availability_zone_hints": [],
      "availability_zones": [
         "az2.dc2",
         "az5.dc5"
      ],
      "admin_state_up": true,
      "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
      "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
      "provider:network_type": "vxlan",
      "router:external": false,
      "port_security_enabled": true,
      "created_at": "2018-09-20T01:53:18",
      "updated_at": "2018-09-20T01:53:20"
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.3.4 Updating a Network

Function

This API is used to update a network.

URI

PUT /v2.0/networks/{network_id}

Table 6-60 describes the parameters.

Table 6-60 Parameter description

Parameter	Mandatory	Description
network_id	Yes	Specifies the network ID.

Request Parameters

Table 6-61 Request parameter

Parameter	Type	Mandatory	Description
network	**network** object	Yes	Specifies the network. For details, see **Table 6-62**. You must specify at least one attribute when updating a network.

Table 6-62 network objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the network name. The name cannot be the same as the **admin_external_net** value (preset network name and cannot be used).

Attribute	Mandatory	Type	Description
admin_state_up	No	Boolean	Specifies the administrative status. The value can only be **true**.
port_security_enabled	No	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping settings of all VMs in the network do not take effect.

Example Request

Change the name of the network whose ID is c360322d-5315-45d7-b7d2-481f98c56edb to **network-test02**.

```
PUT https://{Endpoint}/v2.0/networks/c360322d-5315-45d7-b7d2-481f98c56edb

{
  "network": {
    "name": "network-test02"
  }
}
```

Response Parameters

Table 6-63 Response parameter

Parameter	Type	Description
network	network object	Specifies the network. For details, see Table 6-64.

Table 6-64 network objects

Attribute	Type	Description
status	String	Specifies the network status. The value can be **ACTIVE**, **BUILD**, **DOWN**, or **ERROR**.
subnets	Array of strings	Specifies IDs of the subnets associated with this network. The IDs are in a list. Only one subnet can be associated with each network.

Attribute	Type	Description
name	String	Specifies the network name. The name cannot be the same as the **admin_external_net** value (preset network name and cannot be used).
router:external	Boolean	Specifies whether the network is an external network. The default value is **false**. This is an extended attribute.
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.
tenant_id	String	Specifies the project ID.
shared	Boolean	Specifies whether the network can be shared by different tenants.
id	String	Specifies the network ID. This parameter is not mandatory when you query networks.
provider:network_type	String	Specifies the network type. Only the VXLAN and GENEVE networks are supported. Tenants can only set this parameter to **geneve**. If this parameter is not specified, the network type is automatically set to VXLAN. If the network is preset as **admin_external_net**, this parameter is fixed at **vlan** and cannot be configured. Note: • Set this parameter to **geneve** if you want to create GENEVE networks. • Do not specify this parameter if you want to create VXLAN networks.
availability_zone_hints	Array of strings	Specifies the availability zones available to this network. The current version does not support cross-availability-zone network scheduling.
availability_zones	Array of strings	Specifies the availability zone of this network.
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping settings of all VMs in the network do not take effect.

Attribute	Type	Description
dns_domain	String	Specifies the default private network DNS domain address. The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the network is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the network is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "network": {
        "id": "c360322d-5315-45d7-b7d2-481f98c56edb",
        "name": "network-test02",
        "status": "ACTIVE",
        "shared": false,
        "subnets": [],
        "availability_zone_hints": [],
        "availability_zones": [
            "az2.dc2",
            "az5.dc5"
        ],
        "admin_state_up": true,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "provider:network_type": "vxlan",
        "router:external": false,
        "port_security_enabled": true,
        "created_at": "2018-09-20T01:53:18",
        "updated_at": "2018-09-20T01:55:47"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.3.5 Deleting a Network

Function

This API is used to delete a network.

URI

DELETE /v2.0/networks/{network_id}

Table 6-65 describes the parameters.

Table 6-65 Parameter description

Parameter	Mandatory	Description
network_id	Yes	Specifies the network ID.

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/networks/60c809cb-6731-45d0-ace8-3bf5626421a9
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.4 Subnet

6.4.1 Querying Subnets

Function

This API is used to query all subnets accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query operation. If

the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/subnets

Example:

```
GET https://{Endpoint}/v2.0/subnets?
name={subnet_name}&ip_version={ip_version}&network_id={network_id}&cidr={subnet_cidr_address}&gateway_ip={subnet_gateway}&tenant_id={tenant_id}&enable_dhcp={is_enable_dhcp}
```

Example of querying networks by page

```
GET https://{Endpoint}/v2.0/subnets?limit=2&marker=011fc878-5521-4654-a1ad-f5b0b5820302&page_reverse=False
```

Table 6-66 describes the parameters.

Table 6-66 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the ID is used as the filtering condition.
name	No	String	Specifies that the subnet name is used as the filtering condition.
enable_dhcp	No	Boolean	Specifies whether DHCP is enabled for the subnet is used as the filtering condition. The value can be **true** or **false**.
cidr	No	String	Specifies that the CIDR block is used as the filtering condition.
network_id	No	String	Specifies that the network ID is used as the filtering condition.
ip_version	No	String	Specifies that the IP address version is used as the filtering condition.
gateway_ip	No	String	Specifies that the gateway IP address is used as the filtering condition.
tenant_id	No	String	Specifies that the project ID is used as the filtering condition.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

Example 1

```
GET https://{Endpoint}/v2.0/subnets?limit=1
```

Example 2

```
GET https://{Endpoint}/v2.0/subnets?id=011fc878-5521-4654-a1ad-f5b0b5820322
```


Response Parameters

Table 6-67 Response parameter

Parameter	Type	Description
subnets	Array of **subnet** objects	Specifies the subnet list. For details, see **Table 6-68**.
subnets_links	Array of **subnets_link** objects	Specifies the pagination information. For details, see **Table 6-71**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-68 subnet objects

Attribute	Type	Description
id	String	Specifies the subnet ID. This parameter is not mandatory when you query subnets.
name	String	Specifies the subnet name.
ip_version	Integer	Specifies the IP address version. The value can be **4** (IPv4) or **6** (IPv6).
ipv6_address_mode	String	Specifies the IPv6 addressing mode. Only **dhcpv6-stateful** is supported.
ipv6_ra_mode	String	Specifies the IPv6 route broadcast mode. Only **dhcpv6-stateful** is supported.
network_id	String	Specifies the ID of the network to which the subnet belongs.

Attribute	Type	Description
cidr	String	Specifies the CIDR format. Only the IPv4 addresses in the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 ranges are supported. The subnet mask cannot be greater than 28. This parameter cannot be set if the value of **ip_version** is **6**.
gateway_ip	String	The gateway IP address cannot conflict with IP addresses configured for **allocation_pools**. This attribute cannot be modified.
allocation_pools	Array of **allocation_pool** objects	Specifies available IP address pools. For details, see **Table 6-69**. Example: [{ "start": "10.0.0.2", "end": "10.0.0.251"}] The last three and the first IP addresses in each subnet are the ones reserved by the system. For example, in IPv4 subnet 192.168.1.0/24, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. [{"start": "2001:db8:a583:9::2", "end": "2001:db8:a583:9:ffff:ffff:ffff:fffc"}] In IPv6 subnet 2001:db8:a583:9::/64, IP addresses 2001:db8:a583:9::1, 2001:db8:a583:9:ffff:ffff:ffff:fffd, 2001:db8:a583:9:ffff:ffff:ffff:fffe, and 2001:db8:a583:9:ffff:ffff:ffff:ffff are reserved by the system. By default, the IP addresses reserved by the system are not in the IP address pool specified by **allocation_pool**. When updating an IP address pool, the **allocation_pool** value can contain neither gateway nor broadcast IP addresses.

Attribute	Type	Description
dns_nameservers	Array of strings	Specifies the DNS server address. Example: "dns_nameservers": ["8.xx.xx.8","8.xx.xx.4"]
host_routes	Array of **host_route** objects	Specifies the static VM routes. For details, see **Table 6-70**. Static routes are not supported, and entered information will be ignored.
tenant_id	String	Specifies the project ID.
enable_dhcp	Boolean	Specifies whether to enable the DHCP function. Value **false** indicates that the DHCP function is not enabled. The value can only be **true**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the subnet is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-69 allocation_pool objects

Parameter	Type	Description
start	String	Specifies the start IP address of a network pool.
end	String	Specifies the end IP address of a network pool.

Table 6-70 host_route objects

Parameter	Type	Description
destination	String	Specifies the destination subnet of a route.

Parameter	Type	Description
nexthop	String	Specifies the next-hop IP address of a route.

Table 6-71 subnets_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

Example 1

```
{
   "subnets": [
      {
         "name": "kesmdemeet",
         "cidr": "172.16.236.0/24",
         "id": "011fc878-5521-4654-a1ad-f5b0b5820302",
         "enable_dhcp": true,
         "network_id": "48efad0c-079d-4cc8-ace0-dce35d584124",
         "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "dns_nameservers": [],
         "allocation_pools": [
            {
               "start": "172.16.236.2",
               "end": "172.16.236.251"
            }
         ],
         "host_routes": [],
         "ip_version": 4,
         "gateway_ip": "172.16.236.1",
         "created_at": "2018-03-26T08:23:43",
         "updated_at": "2018-03-26T08:23:44"
      }
   ],
   "subnets_links": [
      {
         "rel": "next",
         "href": "https://{Endpoint}/v2.0/subnets?limit=1&marker=011fc878-5521-4654-a1ad-f5b0b5820302"
      },
      {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/subnets?limit=1&marker=011fc878-5521-4654-a1ad-
f5b0b5820302&page_reverse=True"
      }
   ]
}
```

Example 2

```
{
   "subnets": [
      {
```



```
      "id": "011fc878-5521-4654-a1ad-f5b0b5820322",
      "name": "elb_alpha_vpc0_subnet0_172_16_0_0_24",
      "tenant_id": "0c55e5b2b100d5202ff6c01a2fac4580",
      "network_id": "3053b502-11b2-4599-bcf4-d9d06b6118b2",
         "ip_version": 6,
      "cidr": "2001:db8:a583:a0::/64",
         "subnetpool_id": "cb03d100-8687-4c0a-9441-ea568dcae47d",
      "allocation_pools": [{
         "start": "2001:db8:a583:a0::2",
      "end": "2001:db8:a583:a0:ffff:ffff:ffff:fffc"
      }],
      "gateway_ip": "2001:db8:a583:a0::1",
      "enable_dhcp": true,
      "ipv6_ra_mode": "dhcpv6-stateful",
      "ipv6_address_mode": "dhcpv6-stateful",
      "description": "",
      "dns_nameservers": [],
      "host_routes": [],
      "project_id": "0c55e5b2b100d5202ff6c01a2fac4580",
      "created_at": "2021-07-01T07:59:28",
      "updated_at": "2021-07-01T07:59:28"
      }
   ],
   "subnets_links": [
     {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/subnets?limit=1&id=011fc878-5521-4654-a1ad-
f5b0b5820322&marker=011fc878-5521-4654-a1ad-f5b0b5820302&page_reverse=True"
      }
   ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.4.2 Querying a Subnet

Function

This API is used to query details about a subnet.

URI

GET /v2.0/subnets/{subnet_id}

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/subnets/011fc878-5521-4654-a1ad-f5b0b5820302
```


Response Parameters

Table 6-72 Response parameter

Parameter	Type	Description
subnet	**subnet** object	Specifies the subnet. For details, see **Table 6-73**.

Table 6-73 subnet objects

Attribute	Type	Description
id	String	Specifies the subnet ID. This parameter is not mandatory when you query subnets.
name	String	Specifies the subnet name.
ip_version	Integer	Specifies the IP address version. The value can be **4** (IPv4) or **6** (IPv6).
ipv6_address_mode	String	Specifies the IPv6 addressing mode. Only **dhcpv6-stateful** is supported.
ipv6_ra_mode	String	Specifies the IPv6 route broadcast mode. Only **dhcpv6-stateful** is supported.
network_id	String	Specifies the ID of the network to which the subnet belongs.
cidr	String	Specifies the CIDR format. Only the IPv4 addresses in the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 ranges are supported. The subnet mask cannot be greater than 28. This parameter cannot be set if the value of **ip_version** is **6**.
gateway_ip	String	The gateway IP address cannot conflict with IP addresses configured for **allocation_pools**. This attribute cannot be modified.

Attribute	Type	Description
allocation_pools	Array of **allocation_pool** objects	Specifies the available IP address pool. For details, see **Table 6-74**. Example: [{ "start": "10.0.0.2", "end": "10.0.0.251"}] The last three and the first IP addresses in each subnet are the ones reserved by the system. For example, in subnet **192.168.1.0/24**, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. [{"start": "2001:db8:a583:9::2", "end": "2001:db8:a583:9:ffff:ffff:ffff:fffc"}] In IPv6 subnet 2001:db8:a583:9::/64, IP addresses 2001:db8:a583:9::1, 2001:db8:a583:9:ffff:ffff:ffff:fffd, 2001:db8:a583:9:ffff:ffff:ffff:fffe, and 2001:db8:a583:9:ffff:ffff:ffff:ffff are reserved by the system. By default, the IP addresses reserved by the system are not in the IP address pool specified by **allocation_pool**. When updating an IP address pool, the **allocation_pool** value can contain neither gateway nor broadcast IP addresses.
dns_nameservers	Array of strings	Specifies the DNS server address. Example: "dns_nameservers": ["8.xx.xx.8","8.xx.xx.4"]
host_routes	Array of **host_route** objects	Specifies the static VM routes. For details, see **Table 6-75**. Static routes are not supported, and entered information will be ignored.
tenant_id	String	Specifies the project ID.

Attribute	Type	Description
enable_dhcp	Boolean	Specifies whether to enable the DHCP function. Value **false** indicates that the DHCP function is not enabled. The value can only be **true**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the subnet is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-74 allocation_pool objects

Parameter	Type	Remarks
start	String	Specifies the start IP address of a network pool.
end	String	Specifies the end IP address of a network pool.

Table 6-75 host_route objects

Parameter	Type	Remarks
destination	String	Specifies the destination subnet of a route.
nexthop	String	Specifies the next-hop IP address of a route.

Example Response

```
{
    "subnet": {
        "name": "kesmdemeet",
        "cidr": "172.16.236.0/24",
        "id": "011fc878-5521-4654-a1ad-f5b0b5820302",
        "enable_dhcp": true,
        "network_id": "48efad0c-079d-4cc8-ace0-dce35d584124",
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
```

```
    "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "dns_nameservers": [],
    "allocation_pools": [
      {
        "start": "172.16.236.2",
        "end": "172.16.236.251"
      }
    ],
    "host_routes": [],
    "ip_version": 4,
    "gateway_ip": "172.16.236.1",
    "created_at": "2018-03-26T08:23:43",
    "updated_at": "2018-03-26T08:23:44"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.4.3 Creating a Subnet

Function

This API is used to create a subnet.

URI

POST /v2.0/subnets

Request Parameters

Table 6-76 Request parameter

Parameter	Type	Mandatory	Description
subnet	**subnet** object	Yes	Specifies the subnet. For details, see **Table 6-77**.

Table 6-77 subnet objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the subnet name.
ip_version	No	Integer	Specifies the IP address version. The value can be **4** (IPv4) or **6** (IPv6).

Attribute	Mandatory	Type	Description
ipv6_address_mode	No	String	Specifies the IPv6 addressing mode. Only **dhcpv6-stateful** is supported.
ipv6_ra_mode	No	String	Specifies the IPv6 route broadcast mode. Only **dhcpv6-stateful** is supported.
network_id	Yes	String	Specifies the ID of the network to which the subnet belongs.
cidr	Yes	String	Specifies the CIDR format. Only the IPv4 addresses in the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 ranges are supported. The subnet mask cannot be greater than 28. The IPv6 mask cannot be greater than 128.
gateway_ip	No	String	The gateway IP address cannot conflict with IP addresses configured for **allocation_pools**. This attribute cannot be modified.

Attribute	Mandatory	Type	Description
allocation_pools	No	Array of **allocation_pool** objects	Specifies the available IP address pool. For details, see **Table 6-78**. Example: [{ "start": "10.0.0.2", "end": "10.0.0.251"}] The last three and the first IP addresses in each subnet are the ones reserved by the system. For example, in subnet 192.168.1.0/24, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. [{"start": "2001:db8:a583:9::2", "end": "2001:db8:a583:9:ffff:ffff:ffff:fffc"}] In IPv6 subnet 2001:db8:a583:9::/64, IP addresses 2001:db8:a583:9::1, 2001:db8:a583:9:ffff:ffff:ffff:fffd, 2001:db8:a583:9:ffff:ffff:ffff:fffe, and 2001:db8:a583:9:ffff:ffff:ffff:ffff are reserved by the system. By default, the IP addresses reserved by the system are not in the IP address pool specified by **allocation_pool**. When updating an IP address pool, the **allocation_pool** value can contain neither gateway nor broadcast IP addresses.

Attribute	Mandatory	Type	Description
dns_nameservers	No	Array of strings	Specifies the DNS server address. Instructions: Example: "dns_nameservers": ["8.xx.xx.8","8.xx.xx.4"] A maximum of five DNS server addresses are supported. If this parameter is left empty, the default value is null. For instructions about how to obtain a private DNS server address, see **What Are the Private DNS Server Addresses Provided by the DNS Service?**
host_routes	No	Array of **host_route** objects	Specifies the static VM routes. For details, see **Table 6-79**. Static routes are not supported, and entered information will be ignored.
enable_dhcp	No	Boolean	Specifies whether to enable the DHCP function. Value **false** indicates that the DHCP function is not enabled. The value can only be **true**.

Table 6-78 allocation_pool objects

Parameter	Mandatory	Type	Description
start	No	String	Specifies the start IP address of a network pool.
end	No	String	Specifies the end IP address of a network pool.

Table 6-79 host_route objects

Parameter	Mandatory	Type	Description
destination	No	String	Specifies the destination subnet of a route.
nexthop	No	String	Specifies the next-hop IP address of a route.

Example Request

Create an IPv4 subnet named **subnet-test**, set its network ID to 0133cd73-34d4-4d4c-bf1f-e65b24603206, and CIDR block to 172.16.2.0/24.

```
POST https://{Endpoint}/v2.0/subnets

{
   "subnet": {
        "name": "subnet-test",
        "network_id": "0133cd73-34d4-4d4c-bf1f-e65b24603206",
        "cidr": "172.16.2.0/24",
        "enable_dhcp": true
   }
}
```

Response Parameters

Table 6-80 Response parameter

Parameter	Type	Description
subnet	**subnet** object	Specifies the subnet. For details, see **Table 6-81**.

Table 6-81 subnet objects

Attribute	Type	Description
id	String	Specifies the subnet ID. This parameter is not mandatory when you query subnets.
name	String	Specifies the subnet name.
ip_version	Integer	Specifies the IP address version. The value can be **4** (IPv4) or **6** (IPv6).

Attribute	Type	Description
ipv6_address_mode	String	Specifies the IPv6 addressing mode. Only **dhcpv6-stateful** is supported.
ipv6_ra_mode	String	Specifies the IPv6 route broadcast mode. Only **dhcpv6-stateful** is supported.
network_id	String	Specifies the ID of the network to which the subnet belongs.
cidr	String	Specifies the CIDR format. Only the addresses in the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 ranges are supported. In addition, the subnet mask cannot be greater than 28.
gateway_ip	String	The gateway IP address cannot conflict with IP addresses configured for **allocation_pools**. This attribute cannot be modified.

Attribute	Type	Description
allocation_pools	Array of **allocation_pool** objects	Specifies the available IP address pool. For details, see the **allocation_pool** objects. **Table 6-82** Example: [{ "start": "10.0.0.2", "end": "10.0.0.251"}] The last three and the first IP addresses in each subnet are the ones reserved by the system. For example, in subnet **192.168.1.0/24**, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. By default, the IP addresses reserved by the system are not in the IP address pool specified by **allocation_pool**. [{"start": "2001:db8:a583:9::2", "end": "2001:db8:a583:9:ffff:ffff:ffff:fffc"}] In IPv6 subnet 2001:db8:a583:9::/64, IP addresses 2001:db8:a583:9::1, 2001:db8:a583:9:ffff:ffff:ffff:fffd, 2001:db8:a583:9:ffff:ffff:ffff:fffe, and 2001:db8:a583:9:ffff:ffff:ffff:ffff are reserved by the system. When updating an IP address pool, the **allocation_pool** value can contain neither gateway nor broadcast IP addresses.
dns_nameservers	Array of strings	Specifies the DNS server address. Example: "dns_nameservers": ["8.xx.xx.8","8.xx.xx.4"]
host_routes	Array of **host_route** objects	Specifies the static VM routes. For details, see **Table 6-83**. Static routes are not supported, and entered information will be ignored.
tenant_id	String	Specifies the project ID.

Attribute	Type	Description
enable_dhcp	Boolean	Specifies whether to enable the DHCP function. Value **false** indicates that the DHCP function is not enabled. The value can only be **true**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the subnet is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-82 allocation_pool objects

Parameter	Type	Remarks
start	String	Specifies the start IP address of a network pool.
end	String	Specifies the end IP address of a network pool.

Table 6-83 host_route objects

Parameter	Type	Remarks
destination	String	Specifies the destination subnet of a route.
nexthop	String	Specifies the next-hop IP address of a route.

Example Response

```
{
    "subnet": {
        "name": "subnet-test",
        "cidr": "172.16.2.0/24",
        "id": "98bac90c-0ba7-4a63-8995-097da9bead1c",
        "enable_dhcp": true,
        "network_id": "0133cd73-34d4-4d4c-bf1f-e65b24603206",
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
```



```
    "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "dns_nameservers": [],
    "allocation_pools": [
      {
        "start": "172.16.2.2",
        "end": "172.16.2.251"
      }
    ],
    "host_routes": [],
    "ip_version": 4,
    "gateway_ip": "172.16.2.1",
    "created_at": "2018-09-20T02:02:16",
    "updated_at": "2018-09-20T02:02:16"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.4.4 Updating a Subnet

Function

This API is used to update information about a subnet.

Restrictions

When updating the **allocation_pools** field, neither gateway nor broadcast IP addresses can be included.

URI

PUT /v2.0/subnets/{subnet_id}

Request Parameters

Table 6-84 Request parameter

Parameter	Type	Mandatory	Description
subnet	**subnet** object	Yes	Specifies the subnet. For details, see **Table 6-85**. You must specify at least one attribute when updating a subnet.

Table 6-85 subnet objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the subnet name.
allocation_pools	No	Array of **allocation_pool** objects	Specifies the available IP address pool. For details about the **allocation_pool** objects, see **Table 6-86**. Example: [{ "start": "10.0.0.2", "end": "10.0.0.251"}] The last three and the first IP addresses in each subnet are the ones reserved by the system. For example, in subnet **192.168.1.0/24**, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. By default, the IP addresses reserved by the system are not in the IP address pool specified by **allocation_pool**. [{"start": "2001:db8:a583:9::2", "end": "2001:db8:a583:9:ffff:ffff:ffff:fffc"}] In IPv6 subnet 2001:db8:a583:9::/64, IP addresses 2001:db8:a583:9::1, 2001:db8:a583:9:ffff:ffff:ffff:fffd, 2001:db8:a583:9:ffff:ffff:ffff:fffe, and 2001:db8:a583:9:ffff:ffff:ffff:ffff are reserved by the system. When updating an IP address pool, the **allocation_pool** value can contain neither gateway nor broadcast IP addresses.

Attribute	Mandatory	Type	Description
dns_nameservers	No	Array of strings	Specifies the DNS server address. Instructions: Example: "dns_nameservers": ["8.xx.xx.8","8.xx.xx.4"] A maximum of five DNS server addresses are supported.
host_routes	No	Array of **host_route** objects	Specifies the static VM routes. For details, see **Table 6-87**. Static routes are not supported, and entered information will be ignored.
enable_dhcp	No	Boolean	Specifies whether to enable the DHCP function. Value **false** indicates that the DHCP function is not enabled. The value can only be **true**.

Table 6-86 allocation_pool objects

Parameter	Mandatory	Type	Description
start	No	String	Specifies the start IP address of a network pool.
end	No	String	Specifies the end IP address of a network pool.

Table 6-87 host_route objects

Parameter	Mandatory	Type	Description
destination	No	String	Specifies the destination subnet of a route.
nexthop	No	String	Specifies the next-hop IP address of a route.

Example Request

Change the name of the subnet whose ID is 98bac90c-0ba7-4a63-8995-097da9bead1c to **subnet-test**.

```
PUT https://{Endpoint}/v2.0/subnets/98bac90c-0ba7-4a63-8995-097da9bead1c
{
  "subnet": {
    "name": "subnet-test"
  }
}
```

Response Parameters

Table 6-88 Response parameter

Parameter	Type	Description
subnet	**subnet** object	Specifies the subnet. For details, see **Table 6-89**.

Table 6-89 subnet objects

Attribute	Type	Description
id	String	Specifies the subnet ID. This parameter is not mandatory when you query subnets.
name	String	Specifies the subnet name.
ip_version	Integer	Specifies the IP address version. The value can be **4** (IPv4) or **6** (IPv6).
ipv6_address_mode	String	Specifies the IPv6 addressing mode. Only **dhcpv6-stateful** is supported.
ipv6_ra_mode	String	Specifies the IPv6 route broadcast mode. Only **dhcpv6-stateful** is supported.
network_id	String	Specifies the ID of the network to which the subnet belongs.

Attribute	Type	Description
cidr	String	Specifies the CIDR format. Only the IPv4 addresses in the 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 ranges are supported. The subnet mask cannot be greater than 28. The IPv6 mask cannot be greater than 128.
gateway_ip	String	The gateway IP address cannot conflict with IP addresses configured for **allocation_pools**. This attribute cannot be modified.

Attribute	Type	Description
allocation_pools	Array of **allocation_pool** objects	Specifies the available IP address pool. For details, see the **allocation_pool** objects. **Table 6-90** Example: [{ "start": "10.0.0.2", "end": "10.0.0.251"}] The last three and the first IP addresses in each subnet are the ones reserved by the system. For example, in IPv4 subnet 192.168.1.0/24, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. [{"start": "2001:db8:a583:9::2", "end": "2001:db8:a583:9:ffff:ffff:ffff:fffc"}] In IPv6 subnet 2001:db8:a583:9::/64, IP addresses 2001:db8:a583:9::1, 2001:db8:a583:9:ffff:ffff:ffff:fffd, 2001:db8:a583:9:ffff:ffff:ffff:fffe, and 2001:db8:a583:9:ffff:ffff:ffff:ffff are reserved by the system. By default, the IP addresses reserved by the system are not in the IP address pool specified by **allocation_pool**. When updating an IP address pool, the **allocation_pool** value can contain neither gateway nor broadcast IP addresses.
dns_nameservers	Array of strings	Specifies the DNS server address. Example: "dns_nameservers": ["8.xx.xx.8","8.xx.xx.4"]
host_routes	Array of **host_route** objects	Specifies the static VM routes. For details, see **Table 6-91**. Static routes are not supported, and entered information will be ignored.
tenant_id	String	Specifies the project ID.

Attribute	Type	Description
enable_dhcp	Boolean	Specifies whether to enable the DHCP function. Value **false** indicates that the DHCP function is not enabled. The value can only be **true**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the subnet is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the subnet is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-90 allocation_pool objects

Parameter	Type	Remarks
start	String	Specifies the start IP address of a network pool.
end	String	Specifies the end IP address of a network pool.

Table 6-91 host_route objects

Parameter	Type	Remarks
destination	String	Specifies the destination subnet of a route.
nexthop	String	Specifies the next-hop IP address of a route.

Example Response

```
{
    "subnet": {
        "name": "subnet-test",
        "cidr": "172.16.2.0/24",
        "id": "98bac90c-0ba7-4a63-8995-097da9bead1c",
        "enable_dhcp": true,
        "network_id": "0133cd73-34d4-4d4c-bf1f-e65b24603206",
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
```

```
    "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "dns_nameservers": [],
    "allocation_pools": [
      {
        "start": "172.16.2.2",
        "end": "172.16.2.251"
      }
    ],
    "host_routes": [],
    "ip_version": 4,
    "gateway_ip": "172.16.2.1",
    "created_at": "2018-09-20T02:02:16",
    "updated_at": "2018-09-20T02:03:03"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.4.5 Deleting a Subnet

Function

This API is used to delete a subnet.

URI

DELETE /v2.0/subnets/{subnet_id}

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/subnets/74259164-e63a-4ad9-9c77-a1bd2c9aa187
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.5 Router

6.5.1 Querying Routers

Function

This API is used to query all routers accessible to the tenant submitting the request.

URI

GET /v2.0/routers

Example:

```
GET https://{Endpoint}/v2.0/routers?
id={id}&name={name}&admin_state_up={admin_state_up}&tenant_id={tenant_id}&status={status}
```

Example of querying routers by page

```
GET https://{Endpoint}/v2.0/routers?
limit=2&marker=01ab4be1-4447-45fb-94be-3ee787ed4ebe&page_reverse=False
```

Table 6-92 describes the parameters.

Table 6-92 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the router ID is used as the filtering condition.
admin_state_up	No	Boolean	Specifies that the admin state is used as the filtering condition. The value can be **true** or **false**.
status	No	String	Specifies that the router status is used as the filtering condition. The value can be **ACTIVE**, **DOWN**, or **ERROE**.
tenant_id	No	String	Specifies that the project ID is used as the filtering condition.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/routers?limit=1
```


Response Parameters

Table 6-93 Response parameter

Parameter	Type	Description
routers	Array of **router** objects	Specifies the router list. For details, see **Table 6-94**.
routers_links	Array of **routers_link** objects	Specifies the pagination information. For details, see **Table 6-97**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-94 router objects

Attribute	Type	Description
id	String	Specifies the router ID. This parameter is not mandatory when you query routers.
name	String	Specifies the router name. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.
status	String	Specifies the router status. The value can be **ACTIVE**, **DOWN**, or **ERROR**.
tenant_id	String	Specifies the project ID.
external_gateway_info	**external_gateway_info** object	Specifies the external gateway. This is an extended attribute. For details, see the **external_gateway_info** objects.
routes	Array of **route** objects	Specifies a route list. This is an extended attribute. For details, see **Table 6-96**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Attribute	Type	Description
created_at	String	Specifies the time (UTC) when the router is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the router is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-95 external_gateway_info objects

Attribute	Type	Description
network_id	String	Specifies the UUID of the external network. You can use **GET /v2.0/networks?router:external=True** or run the **neutron net-external-list** command to query information about the external network.
enable_snat	Boolean	Specifies whether the SNAT function is enabled. The default value is **false**.

Table 6-96 route objects

Attribute	Type	Description
destination	String	Specifies the IP address range.
nexthop	String	Specifies the next hop IP address. The IP address can only be one in the subnet associated with the router.

Table 6-97 routers_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response


```
{
   "routers": [
      {
         "id": "01ab4be1-4447-45fb-94be-3ee787ed4ebe",
         "name": "xiaoleizi-tag",
         "status": "ACTIVE",
         "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "admin_state_up": true,
         "external_gateway_info": {
            "network_id": "0a2228f2-7f8a-45f1-8e09-9039e1d09975",
            "enable_snat": false
         },
         "routes": [
            {
               "destination": "0.0.0.0/0",
               "nexthop": "172.16.0.124"
            }
         ],
         "created_at": "2018-03-23T09:26:08",
         "updated_at": "2018-08-24T08:49:53"
      }
   ],
   "routers_links": [
     {
         "rel": "next",
         "href": "https://{Endpoint}/v2.0/routers?limit=1&marker=01ab4be1-4447-45fb-94be-3ee787ed4ebe"
      },
     {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/routers?
limit=1&marker=01ab4be1-4447-45fb-94be-3ee787ed4ebe&page_reverse=True"
      }
   ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.5.2 Querying a Router

Function

This API is used to query details about a router.

URI

GET /v2.0/routers/{router_id}

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/routers/01ab4be1-4447-45fb-94be-3ee787ed4ebe
```


Response Parameters

Table 6-98 Response parameter

Parameter	Type	Description
router	**router** object	Specifies the router. For details, see **Table 6-99**.

Table 6-99 router objects

Attribute	Type	Description
id	String	Specifies the router ID. This parameter is not mandatory when you query routers.
name	String	Specifies the router name. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.
status	String	Specifies the router status. The value can be **ACTIVE**, **DOWN**, or **ERROR**.
tenant_id	String	Specifies the project ID.
external_gateway_info	**external_gateway_info** object	Specifies the external gateway. This is an extended attribute. For details, see the **external_gateway_info** objects.
routes	Array of **route** objects	Specifies a route list. This is an extended attribute. For details, see **Table 6-101**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the router is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the router is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-100 external_gateway_info objects

Attribute	Type	Description
network_id	String	Specifies the UUID of the external network. You can use **GET /v2.0/networks?router:external=True** or run the **neutron net-external-list** command to query information about the external network.
enable_snat	Boolean	Specifies whether the SNAT function is enabled. The default value is **false**.

Table 6-101 route objects

Attribute	Type	Description
destination	String	Specifies the IP address range.
nexthop	String	Specifies the next hop IP address. The IP address can only be one in the subnet associated with the router.

Example Response

```
{
    "router": {
        "id": "01ab4be1-4447-45fb-94be-3ee787ed4ebe",
        "name": "xiaoleizi-tag",
        "status": "ACTIVE",
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "admin_state_up": true,
        "external_gateway_info": {
            "network_id": "0a2228f2-7f8a-45f1-8e09-9039e1d09975",
            "enable_snat": false
        },
        "routes": [
            {
                "destination": "0.0.0.0/0",
                "nexthop": "172.16.0.124"
            }
        ],
        "created_at": "2018-03-23T09:26:08",
        "updated_at": "2018-08-24T08:49:53"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.5.3 Creating a Router

Function

This API is used to create a router.

URI

POST /v2.0/routers

Request Parameters

Table 6-102 Request parameter

Parameter	Type	Mandatory	Description
router	**router** object	Yes	Specifies the router. For details, see **Table 6-103**.

Table 6-103 router objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the router name. Instructions: The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
admin_state_up	No	Boolean	Specifies the administrative status. The value can only be **true**.
external_gateway_info	No	**external_gateway_info** object	Specifies the external gateway. This is an extended attribute. For details, see the **external_gateway_info** objects.

Table 6-104 external_gateway_info objects

Attribute	Mandatory	Type	Description
network_id	No	String	Specifies the UUID of the external network. You can use **GET /v2.0/networks?router:external=True** or run the **neutron net-external-list** command to query information about the external network.

Example Request

Create a router named **router-test2**.

```
POST https://{Endpoint}/v2.0/routers

{
    "router": {
        "name": "router-test2",
        "admin_state_up": true
    }
}
```

Response Parameters

Table 6-105 Response parameter

Parameter	Type	Description
router	**router** object	Specifies the router. For details, see **Table 6-106**.

Table 6-106 router objects

Attribute	Type	Description
id	String	Specifies the router ID. This parameter is not mandatory when you query routers.
name	String	Specifies the router name. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.

Attribute	Type	Description
status	String	Specifies the router status. The value can be **ACTIVE**, **DOWN**, or **ERROR**.
tenant_id	String	Specifies the project ID.
external_gateway_info	**external_gateway_info** object	Specifies the external gateway. This is an extended attribute. For details, see the **external_gateway_info** objects.
routes	Array of **route** objects	Specifies a route list. This is an extended attribute. For details, see **Table 6-108**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the router is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the router is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-107 external_gateway_info objects

Attribute	Type	Description
network_id	String	Specifies the UUID of the external network. You can use **GET /v2.0/networks?router:external=True** or run the **neutron net-external-list** command to query information about the external network.
enable_snat	Boolean	Specifies whether the SNAT function is enabled. The default value is **false**.

Table 6-108 route objects

Attribute	Type	Description
destination	String	Specifies the IP address range.

Attribute	Type	Description
nexthop	String	Specifies the next hop IP address. The IP address can only be one in the subnet associated with the router.

Example Response

```
{
   "router": {
      "id": "f5dbdfe0-86f9-4b0a-9a32-6be143f0a076",
      "name": "router-test2",
      "status": "ACTIVE",
      "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
      "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
      "admin_state_up": true,
      "external_gateway_info": {
         "network_id": "0a2228f2-7f8a-45f1-8e09-9039e1d09975",
         "enable_snat": false
      },
      "routes": [],
      "created_at": "2018-09-20T02:06:07",
      "updated_at": "2018-09-20T02:06:09"
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.5.4 Updating a Router

Function

This API is used to update a router.

URI

PUT /v2.0/routers/{router_id}

Request Parameters

Table 6-109 Request parameter

Parameter	Mandatory	Type	Description
router	Yes	**router** object	Specifies the router. For details, see **Table 6-110**. You must specify at least one attribute when updating a router.

Table 6-110 router objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the router name. Instructions: The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
admin_state_up	No	Boolean	Specifies the administrative status. The value can only be **true**.
external_gateway_info	No	**external_gateway_info** object	Specifies the external gateway. This is an extended attribute. For details, see the **external_gateway_info** objects.
routes	No	Array of **route** objects	Specifies a route list. This is an extended attribute. For details, see **Table 6-112**.

Table 6-111 external_gateway_info objects

Attribute	Mandatory	Type	Description
network_id	No	String	Specifies the UUID of the external network. You can use **GET /v2.0/networks?router:external=True** or run the **neutron net-external-list** command to query information about the external network.

Table 6-112 route objects

Attribute	Mandatory	Type	Description
destination	No	String	Specifies the IP address range. Instructions: The prefix cannot be the same as that of a direct route.

Attribute	Mandatory	Type	Description
nexthop	No	String	Specifies the next hop IP address. The IP address can only be one in the subnet associated with the router.

Example Request

Change the name of the router whose ID is f5dbdfe0-86f9-4b0a-9a32-6be143f0a076 to **router-220**.

```
PUT https://{Endpoint}/v2.0/routers/f5dbdfe0-86f9-4b0a-9a32-6be143f0a076

{
   "router": {
         "name": "router-220"
   }
}
```

Response Parameters

Table 6-113 Response parameter

Parameter	Type	Description
router	**router** object	Specifies the router. For details, see **Table 6-114**.

Table 6-114 router objects

Attribute	Type	Description
id	String	Specifies the router ID. This parameter is not mandatory when you query routers.
name	String	Specifies the router name. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
admin_state_up	Boolean	Specifies the administrative status. The value can only be **true**.
status	String	Specifies the router status. The value can be **ACTIVE**, **DOWN**, or **ERROR**.

Attribute	Type	Description
tenant_id	String	Specifies the project ID.
external_gateway_info	**external_gateway_info** object	Specifies the external gateway. This is an extended attribute. For details, see the **external_gateway_info** objects.
routes	Array of **route** objects	Specifies a route list. This is an extended attribute. For details, see **Table 6-116**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the router is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the router is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-115 external_gateway_info objects

Attribute	Type	Description
network_id	String	Specifies the UUID of the external network. You can use **GET /v2.0/networks?router:external=True** or run the **neutron net-external-list** command to query information about the external network.
enable_snat	Boolean	Specifies whether the SNAT function is enabled. The default value is **false**.

Table 6-116 route objects

Attribute	Type	Description
destination	String	Specifies the IP address range.
nexthop	String	Specifies the next hop IP address. The IP address can only be one in the subnet associated with the router.

Example Response


```
{
    "router": {
        "id": "f5dbdfe0-86f9-4b0a-9a32-6be143f0a076",
        "name": "router-220",
        "status": "ACTIVE",
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "admin_state_up": true,
        "external_gateway_info": {
            "network_id": "0a2228f2-7f8a-45f1-8e09-9039e1d09975",
            "enable_snat": false
        },
        "routes": [],
        "created_at": "2018-09-20T02:06:07",
        "updated_at": "2018-09-20T02:06:09"
    }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.5.5 Deleting a Router

Function

This API is used to delete a router.

URI

DELETE /v2.0/routers/{router_id}

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/routers/0735a367-2caf-48fb-85aa-6082266f342e
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.5.6 Adding an Interface to a Router

Function

This API is used to add an interface to a router.

Restrictions

- When a port is used, the port can have only one IP address.
- When a subnet is used, the gateway IP address must be configured for the subnet.
- A router cannot be added to networks whose **provider:network_type** is **geneve**.
- Only one router can be added to a subnet.

URI

PUT /v2.0/routers/{router_id}/add_router_interface

Request Parameters

Table 6-117 Request parameter

Parameter	Type	Mandatory	Description
subnet_id	String	No	Specifies the subnet ID. Either **subnet_id** or **port_id** is used. Use the gateway IP address of the subnet to create a router interface.
port_id	String	No	Specifies the port ID. Either **subnet_id** or **port_id** is used. Use the port IP address to create a router interface.

Example Request

Add an interface to the router. The router ID is i5b8e885c-1347-4ac2-baf9-2249c8ed1270, and the subnet ID is ab78be2d-782f-42a5-aa72-35879f6890ff.

```
PUT https://{Endpoint}/v2.0/routers/5b8e885c-1347-4ac2-baf9-2249c8ed1270/add_router_interface

{"subnet_id": "ab78be2d-782f-42a5-aa72-35879f6890ff"}
```


Response Parameters

Table 6-118 Response parameter

Parameter	Type	Description
subnet_id	String	Specifies the subnet ID.
tenant_id	String	Specifies the project ID.
project_id	String	Specifies the project ID.
port_id	String	Specifies the port ID.
id	String	Specifies the router ID.

Example Response

```
{
  "subnet_id": "ab78be2d-782f-42a5-aa72-35879f6890ff",
  "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
  "project_id": "6fbe9263116a4b68818cf1edce16bc4f",
  "port_id": "40e86635-b2a3-45de-a7c8-3cced5b7e755",
  "id": "5b8e885c-1347-4ac2-baf9-2249c8ed1270"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.5.7 Removing an Interface from a Router

Function

Removing an interface from a router will also remove the port.

Restrictions

You are not allowed to remove an interface from a router if there are load balancers in the subnet.

URI

PUT /v2.0/routers/{router_id}/remove_router_interface

Request Parameters

Table 6-119 Request parameter

Parameter	Type	Mandatory	Description
subnet_id	String	No	Specifies the subnet ID. Either **subnet_id** or **port_id** must be specified. Use the gateway IP address of the subnet to create a router interface.
port_id	String	No	Specifies the port ID. Either **subnet_id** or **port_id** is used. Use the port IP address to create a router interface.

Example Request

Remove an interface from a router. The router ID is b625c58c-0cfe-49e0-acc8-f2374f8187ff, and the subnet ID is 4b910a10-0860-428b-b463-d84dbc5e288e.

```
PUT https://{Endpoint}/v2.0/routers/b625c58c-0cfe-49e0-acc8-f2374f8187ff/remove_router_interface

{"subnet_id": "4b910a10-0860-428b-b463-d84dbc5e288e"}
```

Response Parameters

Table 6-120 Response parameter

Parameter	Type	Description
subnet_id	String	Specifies the subnet ID.
tenant_id	String	Specifies the project ID.
project_id	String	Specifies the project ID.
port_id	String	Specifies the port ID.
id	String	Specifies the router ID.

Example Response

```
{
  "subnet_id": "4b910a10-0860-428b-b463-d84dbc5e288e",
  "tenant_id": "3d72597871904daeb6887f75f848b531",
  "project_id": "3d72597871904daeb6887f75f848b531",
  "port_id": "34d7d063-8f40-4958-b420-096db40d4067",
  "id": "b625c58c-0cfe-49e0-acc8-f2374f8187ff"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6 Network ACL

6.6.1 Querying Network ACL Rules

Function

This API is used to query all network ACL rules accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/fwaas/firewall_rules

Example:

```
GET https://{Endpoint}/v2.0/fwaas/firewall_rules?
name={firewall_rule_name}&tenant_id={tenant_id}&public={is_public}&protocol={protocol}&ip_version={ip_version}&action={action}&enabled={is_enabled}
```

Example of querying rules by page

```
GET https://{Endpoint}/v2.0/fwaas/firewall_rules?limit=2&marker=2a193015-4a88-4aa1-84ad-d4955adae707&page_reverse=False
```

Table 6-121 describes the parameters.

Table 6-121 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the network ACL rule ID is used as the filtering condition.
name	No	String	Specifies that the network ACL rule name is used as the filtering condition.
description	No	String	Specifies that the network ACL rule description is used as the filtering condition.
ip_version	No	Integer	Specifies that the IP address version is used as the filtering condition. The value can be **4** (IPv4) or **6** (IPv6).

Parameter	Mandatory	Type	Description
action	No	String	Specifies that the network ACL rule action is used as the filtering condition. The value can be **allow** or **deny**.
enabled	No	Boolean	Specifies that the network ACL rule is enabled is used as the filtering condition. The value can be **true** or **false**.
tenant_id	No	String	Specifies that the project ID is used as the filtering condition.
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/fwaas/firewall_rules
```

Response Parameters

Table 6-122 Response parameter

Parameter	Type	Description
firewall_rules	Array of **Firewall Rule** objects	Specifies the firewall rule list. For details, see **Table 6-124**. A maximum of 2000 records can be returned for each query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.
firewall_rules_links	Array of **firewall_rules_link** Object	Specifies the pagination information. For details, see **Table 6-123**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-123 firewall_rules_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Table 6-124 Firewall Rule objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL rule.
name	String	Specifies the network ACL rule name.
description	String	Provides supplementary information about the network ACL rule.
tenant_id	String	Specifies the project ID.
public	Boolean	Specifies whether the firewall rule can be shared by different tenants.
protocol	String	Specifies the IP protocol.
source_port	String	Specifies the source port number or port number range.
destination_port	String	Specifies the destination port number or port number range.
ip_version	Integer	Specifies the IP protocol version.
source_ip_address	String	Specifies the source IP address or CIDR block.
destination_ip_address	String	Specifies the destination IP address or CIDR block.
action	String	Specifies action performed on traffic passing through the network ACL.
enabled	Boolean	Specifies whether the network ACL rule is enabled.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Example Response

```
{
   "firewall_rules": [
      {
         "protocol": "tcp",
         "description": "update check parameter",
         "source_ip_address": "116.66.184.0/24",
         "destination_ip_address": "0.0.0.0/0",
         "destination_port": null,
         "source_port": null,
         "id": "2a193015-4a88-4aa1-84ad-d4955adae707",
         "name": "crhfwruleupdate",
         "tenant_id": "a1c6f90c94334bd2953d9a61b8031a68",
         "project_id": "a1c6f90c94334bd2953d9a61b8031a68",
         "enabled": true,
```



```
            "action": "allow",
            "ip_version": 4,
            "public": false
        },
        {
            "protocol": "tcp",
            "description": "update check parameter",
            "source_ip_address": null,
            "destination_ip_address": null,
            "destination_port": "40:60",
            "source_port": "20:50",
            "id": "db7a204c-9eb1-40a2-9bd6-ed5cfd3cff32",
            "name": "update_firewall-role-tommy",
            "tenant_id": "a1c6f90c94334bd2953d9a61b8031a68",
            "project_id": "a1c6f90c94334bd2953d9a61b8031a68",
            "enabled": false,
            "action": "deny",
            "ip_version": 4,
            "public": false
        }
    ],
    "firewall_rules_links": [
        {    "rel": "previous",
            "href": "https://{Endpoint}/v2.0/fwaas/firewall_rules?marker=2a193015-4a88-4aa1-84ad-
d4955adae707&page_reverse=True"
        }
    ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.2 Querying a Network ACL Rule

Function

This API is used to query details about a specific network ACL rule.

URI

GET /v2.0/fwaas/firewall_rules/{firewall_rule_id}

Table 6-125 describes the parameters.

Table 6-125 Parameter description

Parameter	Mandatory	Type	Description
firewall_rule_id	Yes	String	Specifies the network ACL rule ID, which uniquely identifies the network ACL rule. The **firewall_rule_id** value is used as the filter.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/fwaas/firewall_rules/514e6776-162a-4b5d-ab8b-aa36b86655ef
```

Response Parameters

Table 6-126 Response parameter

Parameter	Type	Description
firewall_rule	**firewall_rule** object	Specifies the firewall rule objects. For details, see **Table 6-127**.

Table 6-127 Firewall Rule objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL rule.
name	String	Specifies the network ACL rule name.
description	String	Provides supplementary information about the network ACL rule.
tenant_id	String	Specifies the project ID.
public	Boolean	Specifies whether the firewall rule can be shared by different tenants.
protocol	String	Specifies the IP protocol.
source_port	String	Specifies the source port number or port number range.
destination_port	String	Specifies the destination port number or port number range.
ip_version	Integer	Specifies the IP protocol version.
source_ip_address	String	Specifies the source IP address or CIDR block.
destination_ip_address	String	Specifies the destination IP address or CIDR block.
action	String	Specifies action performed on traffic passing through the network ACL.

Attribute	Type	Description
enabled	Boolean	Specifies whether the network ACL rule is enabled.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Example Response

```
{
    "firewall_rule": {
        "protocol": "tcp",
        "description": "update check parameter",
        "source_ip_address": "116.66.184.0/24",
        "destination_ip_address": "0.0.0.0/0",
        "destination_port": null,
        "source_port": null,
        "id": "514e6776-162a-4b5d-ab8b-aa36b86655ef",
        "name": "test",
        "tenant_id": "a1c6f90c94334bd2953d9a61b8031a68",
        "project_id": "a1c6f90c94334bd2953d9a61b8031a68",
        "enabled": true,
        "action": "allow",
        "ip_version": 4,
        "public": false
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.3 Creating a Network ACL Rule

Function

This API is used to create a network ACL rule.

URI

POST /v2.0/fwaas/firewall_rules

Request Parameters

Table 6-128 Request parameter

Parameter	Mandatory	Type	Description
firewall_rule	Yes	**firewall_rule** object	Specifies the firewall rule objects. For details, see **Table 6-129**.

Table 6-129 Firewall Rule objects

Attribute	Mandatory	Type	Constraint	Description
name	No	String	The value can contain a maximum of 255 characters.	Specifies the network ACL rule name. The value can contain a maximum of 255 characters.
description	No	String	The value can contain a maximum of 255 characters.	Provides supplementary information about the network ACL rule. The value can contain a maximum of 255 characters.
protocol	No	String	The value can be **TCP**, **UDP**, or **ICMP**.	Specifies the IP protocol. The value can be **TCP**, **UDP**, or **ICMP**.
source_port	No	String	The value can be an integer from 1 to 65535 or a port number range in the format of ***a*:*b***.	Specifies the source port number or port number range. The value can be an integer from 1 to 65535 or a port number range in the format of ***a*:*b***.
destination_port	No	String	The value can be an integer from 1 to 65535 or a port number range in the format of ***a*:*b***.	Specifies the destination port number or port number range. The value can be an integer from 1 to 65535 or a port number range in the format of ***a*:*b***.

Attribute	Mandatory	Type	Constraint	Description
ip_version	No	Integer	4/6	Specifies the IP protocol version. The value can be **4** and **6**, indicating IPv4 address and IPv6 address, respectively.
source_ip_address	No	String	N/A	Specifies the source IP address or CIDR block.
destination_ip_address	No	String	N/A	Specifies the destination IP address or CIDR block.
action	No	String	deny/allow	Specifies action performed on traffic passing through the network ACL. The value can be **deny** or **allow**.
enabled	No	Boolean	The value can be **true** or **false**.	Specifies whether the network ACL rule is enabled. The value can be **true** or **false**.

Example Request

Create an ACL rule with **action** set to **allow**, **protocol** set to **tcp**, and destination port set to 80.

```
POST https://{Endpoint}/v2.0/fwaas/firewall_rules

{
    "firewall_rule": {
        "action": "allow",
        "enabled": true,
        "destination_port": "80",
        "protocol": "tcp",
        "name": "ALLOW_HTTP"
    }
}
```


Response Parameters

Table 6-130 Response parameter

Parameter	Type	Description
firewall_rule	**firewall_rule** object	Specifies the firewall rule objects. For details, see **Table 6-131**.

Table 6-131 Firewall Rule objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL rule.
name	String	Specifies the network ACL rule name.
description	String	Provides supplementary information about the network ACL rule.
tenant_id	String	Specifies the project ID.
public	Boolean	Specifies whether the firewall rule can be shared by different tenants.
protocol	String	Specifies the IP protocol.
source_port	String	Specifies the source port number or port number range.
destination_port	String	Specifies the destination port number or port number range.
ip_version	Integer	Specifies the IP protocol version.
source_ip_address	String	Specifies the source IP address or CIDR block.
destination_ip_address	String	Specifies the destination IP address or CIDR block.
action	String	Specifies action performed on traffic passing through the network ACL.
enabled	Boolean	Specifies whether the network ACL rule is enabled.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Example Response

```
{
    "firewall_rule": {
        "protocol": "tcp",
        "description": "",
        "source_ip_address": null,
        "destination_ip_address": null,
        "source_port": null,
        "destination_port": "80",
        "id": "b94acf06-efc2-485d-ba67-a61acf2a7e28",
        "name": "ALLOW_HTTP",
        "tenant_id": "23c8a121505047b6869edf39f3062712",
        "enabled": true,
        "action": "allow",
        "ip_version": 4,
        "public": false,
        "project_id": "23c8a121505047b6869edf39f3062712"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.4 Updating a Network ACL Rule

Function

This API is used to update a network ACL rule.

URI

PUT /v2.0/fwaas/firewall_rules/{firewall_rule_id}

Request Parameters

Table 6-132 Request parameter

Parameter	Type	Mandatory	Description
firewall_rule	**firewall_rule** object	Yes	Specifies the firewall rule objects. For details, see **Table 6-133**.

Table 6-133 Firewall Rule objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the network ACL rule name. The value can contain a maximum of 255 characters.
description	No	String	Provides supplementary information about the network ACL rule. The value can contain a maximum of 255 characters.
protocol	No	String	Specifies the IP protocol. The value can be **TCP**, **UDP**, **ICMP**, or a value ranging from 0 to 255.
source_port	No	String	Specifies the source port number or port number range. The value can be an integer from 1 to 65535 or a port number range in the format of ***a*:*b***.
destination_port	No	String	Specifies the destination port number or port number range. The value can be an integer from 1 to 65535 or a port number range in the format of ***a*:*b***.
ip_version	No	Integer	Specifies the IP protocol version. The value can be **4** and **6**, indicating IPv4 address and IPv6 address, respectively.
source_ip_address	No	String	Specifies the source IP address or CIDR block.
destination_ip_address	No	String	Specifies the destination IP address or CIDR block.
action	No	String	Specifies action performed on traffic passing through the network ACL. The value can be **deny** or **allow**.

Attribute	Mandatory	Type	Description
enabled	No	Boolean	Specifies whether the network ACL rule is enabled. The value can be **true** or **false**.

Example Request

Change the **action** of the ACL rule whose ID is b94acf06-efc2-485d-ba67-a61acf2a7e28 to **deny**.

```
PUT https://{Endpoint}/v2.0/fwaas/firewall_rules/b94acf06-efc2-485d-ba67-a61acf2a7e28

{
    "firewall_rule": {
        "action": "deny"
    }
}
```

Response Parameters

Table 6-134 Response parameter

Parameter	Type	Description
firewall_rule	**firewall_rule** object	Specifies the firewall rule objects. For details, see **Table 6-135**.

Table 6-135 Firewall Rule objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL rule.
name	String	Specifies the network ACL rule name.
description	String	Provides supplementary information about the network ACL rule.
tenant_id	String	Specifies the project ID.
public	Boolean	Specifies whether the firewall rule can be shared by different tenants.
protocol	String	Specifies the IP protocol.
source_port	String	Specifies the source port number or port number range.

Attribute	Type	Description
destination_port	String	Specifies the destination port number or port number range.
ip_version	Integer	Specifies the IP protocol version.
source_ip_address	String	Specifies the source IP address or CIDR block.
destination_ip_address	String	Specifies the destination IP address or CIDR block.
action	String	Specifies action performed on traffic passing through the network ACL.
enabled	Boolean	Specifies whether the network ACL rule is enabled.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Example Response

```
{
    "firewall_rule": {
        "protocol": "tcp",
        "description": "",
        "source_ip_address": null,
        "destination_ip_address": null,
        "source_port": null,
        "destination_port": "80",
        "id": "b94acf06-efc2-485d-ba67-a61acf2a7e28",
        "name": "ALLOW_HTTP",
        "tenant_id": "23c8a121505047b6869edf39f3062712",
        "enabled": true,
        "action": "deny",
        "ip_version": 4,
        "public": false,
        "project_id": "23c8a121505047b6869edf39f3062712"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.5 Deleting a Network ACL Rule

Function

This API is used to delete a network ACL rule.

NOTE

Before deleting a rule, you need to remove the rule from the corresponding policy first. For details, see **Removing a Network ACL Rule**.

URI

DELETE /v2.0/fwaas/firewall_rules/{firewall_rule_id}

Table 6-136 describes the parameters.

Table 6-136 Parameter description

Parameter	Mandatory	Type	Description
firewall_rule_id	Yes	String	Specifies the network ACL rule ID, which uniquely identifies the network ACL rule.

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/fwaas/firewall_rules/b94acf06-efc2-485d-ba67-a61acf2a7e28
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.6 Querying Network ACL Policies

Function

This API is used to query all network ACL policies accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each

query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/fwaas/firewall_policies

Example of querying policies by page

```
GET https://{Endpoint}/v2.0/fwaas/firewall_policies?limit=2&marker=6b70e321-0c21-4b83-bb8a-a886d1414a5f&page_reverse=False
```

Table 6-137 describes the parameters.

Table 6-137 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the network ACL policy ID is used as the filtering condition.
name	No	String	Specifies that the network ACL policy name is used as the filtering condition.
description	No	String	Specifies that the network ACL policy description is used as the filtering condition.
tenant_id	No	String	Specifies that the project ID of the network ACL policy is used as the filtering condition.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/fwaas/firewall_policies
```

Response Parameters

Table 6-138 Response parameter

Parameter	Type	Description
firewall_policies	Array of **firewall Policy** object	Specifies the firewall policies. For details, see **Table 6-139**.
firewall_policies_links	Array of **firewall_policies_link** object	**firewall_policies_link** object For details, see **Table 6-140**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-139 firewall_Policy object

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL policy.
name	String	Specifies the name of the network ACL policy.
description	String	Provides supplementary information about the network ACL policy.
tenant_id	String	Specifies the project ID.
firewall_rules	Array of strings	Specifies the rules referenced by the network ACL policy.
audited	Boolean	Specifies the audit flag.
public	Boolean	Specifies whether the policy can be shared by different tenants.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Table 6-140 firewall_policies_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

```
{
   "firewall_policies": [
      {
         "description": "",
         "firewall_rules": [
            "6c6803e0-ca8c-4aa9-afb3-4f89275b6c32"
         ],
         "tenant_id": "23c8a121505047b6869edf39f3062712",
         "public": false,
         "id": "6b70e321-0c21-4b83-bb8a-a886d1414a5f",
         "audited": false,
         "name": "fwp1",
         "project_id": "23c8a121505047b6869edf39f3062712"
      },
      {
         "description": "",
         "firewall_rules": [
            "6c6803e0-ca8c-4aa9-afb3-4f89275b6c32"
         ],
         "tenant_id": "23c8a121505047b6869edf39f3062712",
         "public": false,
         "id": "fce92002-5a15-465d-aaca-9b44453bb738",
         "audited": false,
         "name": "fwp2",
         "project_id": "23c8a121505047b6869edf39f3062712"
      }
   ],
   "firewall_policies_links": [
      {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/fwaas/firewall_policies?marker=6b70e321-0c21-4b83-bb8a-
a886d1414a5f&page_reverse=True"
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.7 Querying a Network ACL Policy

Function

This API is used to query details about a specific network ACL policy.

URI

GET /v2.0/fwaas/firewall_policies/{firewall_policy_id}

Table 6-141 describes the parameters.

Table 6-141 Parameter description

Parameter	Mandatory	Type	Description
firewall_policy_id	Yes	String	Specifies the network ACL policy ID, which uniquely identifies the network ACL policy. The **firewall_policy_id** value is used as the filter.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/fwaas/firewall_policies/fed2d88f-d0e7-4cc5-bd7e-c495f67037b6
```

Response Parameters

Table 6-142 Response parameter

Parameter	Type	Description
firewall_policy	**firewall_policy** object	Specifies the firewall policy. For details, see Table 6-143.

Table 6-143 Firewall Policy objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL policy.
name	String	Specifies the name of the network ACL policy.

Attribute	Type	Description
description	String	Provides supplementary information about the network ACL policy.
tenant_id	String	Specifies the project ID.
firewall_rules	Array of strings	Specifies the firewall rules referenced by the network ACL policy.
audited	Boolean	Specifies the audit flag.
public	Boolean	Specifies whether the firewall policy can be shared by different tenants.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Example Response

```
{
    "firewall_policy": {
        "description": "",
        "firewall_rules": [
            "3c0e6267-73df-4d9a-87a6-e226f2db2036"
        ],
        "tenant_id": "23c8a121505047b6869edf39f3062712",
        "public": false,
        "id": "fed2d88f-d0e7-4cc5-bd7e-c495f67037b6",
        "audited": false,
        "name": "bobby_fwp1",
        "project_id": "23c8a121505047b6869edf39f3062712"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.8 Creating a Network ACL Policy

Function

This API is used to create a network ACL policy which must be bound to a network ACL group. You can learn more about the **relationships among network ACL groups, policies, and rules**.

URI

POST /v2.0/fwaas/firewall_policies

Request Parameters

Table 6-144 Request parameter

Parameter	Type	Mandatory	Description
firewall_policy	**firewall_policy** object	Yes	Specifies the firewall policy. For details, see **Table 6-145**.

Table 6-145 Firewall Policy objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the name of the network ACL policy. The value can contain a maximum of 255 characters.
description	No	String	Provides supplementary information about the network ACL policy. The value can contain a maximum of 255 characters.
firewall_rules	No	Array of strings	Specifies the firewall rules referenced by the network ACL policy.
audited	No	Boolean	Specifies the audit flag. The value can be **true** or **false**.

Example Request

Create an ACL policy named **test-policy** and associate it with the ACL rule whose ID is b8243448-cb3c-496e-851c-dadade4c161b.

```
POST https://{Endpoint}/v2.0/fwaas/firewall_policies

{
    "firewall_policy": {
        "name": "test-policy",
        "firewall_rules": [
            "b8243448-cb3c-496e-851c-dadade4c161b"
        ]
    }
}
```

Response Parameters

Table 6-146 Response parameter

Parameter	Type	Description
firewall_policy	**firewall_policy** object	Specifies the firewall policy. For details, see **Table 6-147**.

Table 6-147 Firewall Policy objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL policy.
name	String	Specifies the name of the network ACL policy.
description	String	Provides supplementary information about the network ACL policy.
tenant_id	String	Specifies the project ID.
firewall_rules	Array of strings	Specifies the firewall rules referenced by the network ACL policy.
audited	Boolean	Specifies the audit flag.
public	Boolean	Specifies whether the firewall policy can be shared by different tenants.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Example Response

```
{
    "firewall_policy": {
        "description": "",
        "firewall_rules": [
            "b8243448-cb3c-496e-851c-dadade4c161b"
        ],
        "tenant_id": "23c8a121505047b6869edf39f3062712",
        "public": false,
        "id": "2fb0e81f-9f63-44b2-9894-c13a3284594a",
        "audited": false,
        "name": "test-policy",
        "project_id": "23c8a121505047b6869edf39f3062712"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.9 Updating a Network ACL Policy

Function

This API is used to update a network ACL policy.

URI

PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}

Request Parameters

Table 6-148 Request parameter

Parameter	Type	Mandatory	Description
firewall_policy	**firewall_policy** object	Yes	Specifies the firewall policy objects. For details, see **Table 6-149**.

Table 6-149 Firewall Policy objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the name of the network ACL policy. The value can contain a maximum of 255 characters.
description	No	String	Provides supplementary information about the network ACL policy. The value can contain a maximum of 255 characters.
firewall_rules	No	Array of strings	Specifies the firewall rules referenced by the network ACL policy.
audited	No	Boolean	Specifies the audit flag. The value can be **true** or **false**.

Example Request

Associate the ACL policy whose ID is 2fb0e81f-9f63-44b2-9894-c13a3284594a to the ACL rule whose ID is 0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1.

```
PUT https://{Endpoint}/v2.0/fwaas/firewall_policies/2fb0e81f-9f63-44b2-9894-c13a3284594a

{
   "firewall_policy": {
      "firewall_rules": [
         "0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1"
      ]
   }
}
```

Response Parameters

Table 6-150 Response parameter

Parameter	Type	Description
firewall_policy	**firewall_policy** object	Specifies the firewall policy objects. For details, see **Table 6-151**.

Table 6-151 Firewall Policy objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL policy.
name	String	Specifies the name of the network ACL policy.
description	String	Provides supplementary information about the network ACL policy.
tenant_id	String	Specifies the project ID.
firewall_rules	Array of strings	Specifies the firewall rules referenced by the network ACL policy.
audited	Boolean	Specifies the audit flag.
public	Boolean	Specifies whether the firewall policy can be shared by different tenants.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.

Example Response

```
{
   "firewall_policy": {
      "description": "",
      "firewall_rules": [
         "0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1"
      ],
      "tenant_id": "23c8a121505047b6869edf39f3062712",
      "public": false,
      "id": "2fb0e81f-9f63-44b2-9894-c13a3284594a",
      "audited": false,
      "name": "test-policy",
      "project_id": "23c8a121505047b6869edf39f3062712"
   }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.10 Deleting a Network ACL Policy

Function

This API is used to delete a network ACL policy.

URI

DELETE /v2.0/fwaas/firewall_policies/{firewall_policy_id}

Table 6-152 describes the parameters.

Table 6-152 Parameter description

Parameter	Mandatory	Type	Description
firewall_policy_id	Yes	String	Specifies the network ACL policy ID, which uniquely identifies the network ACL policy.

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/fwaas/firewall_policies/2fb0e81f-9f63-44b2-9894-c13a3284594a
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.11 Inserting a Network ACL Rule

Function

This API is used to insert a network ACL rule to a network ACL policy.

URI

PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}/insert_rule

Table 6-153 describes the parameters.

Table 6-153 Parameter description

Parameter	Mandatory	Type	Description
firewall_policy_id	Yes	String	Specifies the network ACL policy ID, which uniquely identifies the network ACL policy.

Request Parameters

Table 6-154 Request parameter

Parameter	Type	Mandatory	Description
firewall_rule_id	String	Yes	Specifies the network ACL rule ID, which uniquely identifies the network ACL rule.

Parameter	Type	Mandatory	Description
insert_after	String	No	The **insert_after** parameter indicates the firewall rule that has already been associated with the firewall policy. A new firewall rule will be inserted after the firewall rule associated with the firewall policy. If both the **insert_after** and **insert_before** parameters are specified, the **insert_after** parameter will be ignored.
insert_before	String	No	The **insert_before** parameter indicates the firewall rule that has already been associated with the firewall policy. A new firewall rule will be inserted before the firewall rule associated with the firewall policy. If both the **insert_after** and **insert_before** parameters are specified, the **insert_after** parameter will be ignored.

Example Request

Insert rule 0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1 below rule b8243448-cb3c-496e-851c-dadade4c161b in the ACL policy whose ID is afc52ce9-5305-4ec9-9feb-44feb8330341.

```
PUT https://{Endpoint}/v2.0/fwaas/firewall_policies/afc52ce9-5305-4ec9-9feb-44feb8330341/insert_rule

{
    "insert_after": "b8243448-cb3c-496e-851c-dadade4c161b",
    "firewall_rule_id": "0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1",
    "insert_before": ""
}
```

Response Parameters

Table 6-155 Response parameter

Parameter	Type	Description
description	String	Provides supplementary information about the firewall policy.
audited	Boolean	Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to **False**.

Parameter	Type	Description
firewall_rules	Array of strings	Specifies the ID list of the firewall rules associated with the current firewall policy.
id	String	Specifies the firewall policy ID.
name	String	Specifies the firewall policy name.
public	Boolean	If this attribute is set to **true**, the network ACL policy is visible to tenants other than its owner. The network ACL policy is not visible to other tenants by default.
tenant_id	String	Specifies the project ID.
project_id	String	Specifies the project ID.

Example Response

```
{
    "description": "",
    "firewall_rules": [
        "b8243448-cb3c-496e-851c-dadade4c161b",
        "0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1"
    ],
    "tenant_id": "23c8a121505047b6869edf39f3062712",
    "public": false,
    "id": "afc52ce9-5305-4ec9-9feb-44feb8330341",
    "audited": false,
    "name": "test-policy",
    "project_id": "23c8a121505047b6869edf39f3062712"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.12 Removing a Network ACL Rule

Function

This API is used to remove a network ACL rule from a network ACL policy.

URI

PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}/remove_rule

Request Parameters

Table 6-156 Request parameter

Parameter	Type	Mandatory	Description
firewall_rule_id	String	Yes	Specifies the network ACL rule ID, which uniquely identifies the network ACL rule.

Example Request

Remove ACL rule 0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1 from the ACL policy whose ID is afc52ce9-5305-4ec9-9feb-44feb8330341.

```
PUT https://{Endpoint}/v2.0/fwaas/firewall_policies/afc52ce9-5305-4ec9-9feb-44feb8330341/remove_rule

{
   "firewall_rule_id": "0f82b221-8cd6-44bd-9dfc-0e118fa7b6b1"
}
```

Response Parameters

Table 6-157 Response parameter

Parameter	Type	Description
description	String	Provides supplementary information about the firewall policy.
audited	Boolean	Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to **False**.
firewall_rules	Array of strings	Specifies the ID list of the firewall rules associated with the current firewall policy.
id	String	Specifies the firewall policy ID.
name	String	Specifies the firewall policy name.
public	Boolean	If this attribute is set to **true**, the network ACL policy is visible to tenants other than its owner. The network ACL policy is not visible to other tenants by default.
tenant_id	String	Specifies the project ID.
project_id	String	Specifies the project ID.

Example Response

```
{
    "description": "",
    "firewall_rules": [
        "b8243448-cb3c-496e-851c-dadade4c161b"
    ],
    "tenant_id": "23c8a121505047b6869edf39f3062712",
    "public": false,
    "id": "afc52ce9-5305-4ec9-9feb-44feb8330341",
    "audited": false,
    "name": "test-policy",
    "project_id": "23c8a121505047b6869edf39f3062712"
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.13 Querying Network ACL Groups

Function

This API is used to query all network ACL groups accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/fwaas/firewall_groups

Example of querying groups by page

```
GET https://{Endpoint}/v2.0/fwaas/firewall_groups?
limit=2&marker=cd600d47-0045-483f-87a1-5041ae2f513b&page_reverse=False
```

Table 6-158 describes the parameters.

Table 6-158 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the ID of the network ACL group is used as the filtering condition.
name	No	String	Specifies that the name of the network ACL group is used as the filtering condition.

Parameter	Mandatory	Type	Description
description	No	String	Specifies that the description of the network ACL group is used as the filtering condition.
admin_state_up	No	Boolean	Specifies that the admin state of the network ACL group is used as the filtering condition. The value can be **true** or **false**.
tenant_id	No	String	Specifies that the project ID of the network ACL group is used as the filtering condition.
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. ● If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. ● If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. ● If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. ● If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/fwaas/firewall_groups
```

Response Parameters

Table 6-159 Response parameter

Parameter	Type	Description
firewall_groups	Array of **Firewall Group** objects	Specifies the firewall group list. For details, see **Table 6-160**.
firewall_groups_links	Array of **firewall_groups_link** objects	Specifies the **firewall_groups_link** object list. For details, see **Table 6-161**. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-160 Firewall Group objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL group.
name	String	Specifies the name of the network ACL group.

Attribute	Type	Description
description	String	Provides supplementary information about the network ACL group.
tenant_id	String	Specifies the project ID.
ingress_firewall_policy_id	String	Specifies the network ACL policy for inbound traffic.
egress_firewall_policy_id	String	Specifies the network ACL policy for outbound traffic.
ports	Array of strings	Specifies the list of ports bound with the network ACL group.
public	Boolean	Specifies whether the firewall group can be shared by different tenants.
status	String	Specifies the status of a network ACL group. The value can be: • **ACTIVE** (Normal) • **INACTIVE** (Inactive) • **ERROR** (Error occurred) • **PENDING_CREATE** (Creating) • **PENDING_UPDATE** (Updating) • **PENDING_DELETE** (Deleting)
admin_state_up	Boolean	Specifies the administrative status of the network ACL.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the resource is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-161 firewall_groups_link object

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response

```
{
   "firewall_groups": [
      {
         "status": "INACTIVE",
         "public": false,
         "egress_firewall_policy_id": null,
         "name": "",
         "admin_state_up": true,
         "ports": [ ],
         "tenant_id": "23c8a121505047b6869edf39f3062712",
         "id": "cd600d47-0045-483f-87a1-5041ae2f513b",
         "ingress_firewall_policy_id": null,
         "description": "",
         "project_id": "23c8a121505047b6869edf39f3062712",
         "created_at": "2018-09-12T08:24:14",
         "updated_at": "2018-09-12T08:24:14"
      },
      {
         "status": "INACTIVE",
         "public": false,
         "egress_firewall_policy_id": "d939df29-fe76-4089-90c3-3778e4d53141",
         "name": "fwg-1475475043",
         "admin_state_up": true,
         "ports": [ ],
         "tenant_id": "0af57070695044ea9a70f04779e6aa1f",
         "id": "ca971b45-70ce-4879-9734-b6cac1d00845",
         "ingress_firewall_policy_id": "d939df29-fe76-4089-90c3-3778e4d53141",
         "description": "",
         "project_id": "0af57070695044ea9a70f04779e6aa1f",
         "created_at": "2018-09-12T08:24:14",
         "updated_at": "2018-09-12T08:24:14"
      }
   ],
   "firewall_groups_links": [
     {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/fwaas/firewall_groups?
marker=cd600d47-0045-483f-87a1-5041ae2f513b&page_reverse=True"
      }
   ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.14 Querying a Network ACL Group

Function

This API is used to query details about a specific network ACL group.

URI

GET /v2.0/fwaas/firewall_groups/{firewall_group_id}

Table 6-162 describes the parameters.

Table 6-162 Parameter description

Parameter	Mandatory	Type	Description
firewall_group_id	Yes	String	Specifies the network ACL group ID, which uniquely identifies the network ACL group. The **fire_group_id** value is used as the filter.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/fwaas/firewall_groups/a504a4cf-9300-40e0-b2d4-649bd157c55a
```

Response Parameters

Table 6-163 Response parameter

Parameter	Type	Description
firewall_group	**firewall_group** object	Specifies the firewall group. For details, see Table 6-164.

Table 6-164 Firewall Group objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL group.
name	String	Specifies the name of the network ACL group.

Attribute	Type	Description
description	String	Provides supplementary information about the network ACL group.
tenant_id	String	Specifies the project ID.
ingress_firewall_policy_id	String	Specifies the network ACL policy for inbound traffic.
egress_firewall_policy_id	String	Specifies the network ACL policy for outbound traffic.
ports	Array of strings	Specifies the list of ports bound with the network ACL group.
public	Boolean	Specifies whether the firewall group can be shared by different tenants.
status	String	Specifies the status of the network ACL policy. The value can be: • **ACTIVE** (Normal) • **INACTIVE** (Inactive) • **ERROR** (Error occurred) • **PENDING_CREATE** (Creating) • **PENDING_UPDATE** (Updating) • **PENDING_DELETE** (Deleting)
admin_state_up	Boolean	Specifies the administrative status of the network ACL.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the resource is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "firewall_group": {
        "status": "ACTIVE",
```



```
    "public": false,
    "egress_firewall_policy_id": null,
    "name": "bobby_fwg1",
    "admin_state_up": true,
    "ports": [
        "16e6d779-15e9-48fb-abc5-b86457792a15"
    ],
    "tenant_id": "23c8a121505047b6869edf39f3062712",
    "id": "a504a4cf-9300-40e0-b2d4-649bd157c55a",
    "ingress_firewall_policy_id": "fed2d88f-d0e7-4cc5-bd7e-c495f67037b6",
    "description": "test",
    "project_id": "23c8a121505047b6869edf39f3062712",
    "created_at": "2018-09-12T08:24:14",
    "updated_at": "2018-09-12T08:24:14"
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.15 Creating a Network ACL Group

Function

This API is used to create a network ACL group.

URI

POST /v2.0/fwaas/firewall_groups

Request Parameters

Table 6-165 Request parameter

Parameter	Type	Mandatory	Description
firewall_group	**firewall_group** object	Yes	Specifies the firewall group. For details, see **Table 6-166**.

Table 6-166 Firewall Group objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the name of the network ACL group. The value can contain a maximum of 255 characters.

Attribute	Mandatory	Type	Description
description	No	String	Provides supplementary information about the network ACL group. The value can contain a maximum of 255 characters.
ingress_firewall_policy_id	No	String	Specifies the network ACL policy for inbound traffic.
egress_firewall_policy_id	No	String	Specifies the network ACL policy for outbound traffic.
ports	No	Array of strings	Specifies the list of ports bound with the network ACL group. The value must be the port ID. **NOTE** The port is the one whose **device_owner** is **network:router_interface_distributed**. • Call the VPC API for querying the port ID. For details, see **Querying Ports**. The filtering criteria are the specified **network_id** and **device_owner**. The **network_id** is the network ID of the subnet associated with the network ACL. Example: GET https://{Endpoint}/v1/{project_id}/ports?network_id={network_id}&device_owner=network%3Arouter_interface_distributed
admin_state_up	No	Boolean	Specifies the administrative status of the network ACL. The value can be **true** or **false**.

Example Request

Create an ACL group, associate it with the inbound ACL policy afc52ce9-5305-4ec9-9feb-44feb8330341, and set the port ID to c133f2bf-6937-4416-bb17-012e1be5cd2d.

```
POST https://{Endpoint}/v2.0/fwaas/firewall_groups

{
    "firewall_group": {
        "name": "test",
```



```
    "ingress_firewall_policy_id": "afc52ce9-5305-4ec9-9feb-44feb8330341",
    "ports": [
      "c133f2bf-6937-4416-bb17-012e1be5cd2d"
    ]
  }
}
```

Response Parameters

Table 6-167 Response parameter

Parameter	Type	Description
firewall_group	**firewall_group** object	Specifies the firewall group. For details, see **Table 6-168**.

Table 6-168 Firewall Group objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL group.
name	String	Specifies the name of the network ACL group.
description	String	Provides supplementary information about the network ACL group.
tenant_id	String	Specifies the project ID.
ingress_firewall_policy_id	String	Specifies the network ACL policy for inbound traffic.
egress_firewall_policy_id	String	Specifies the network ACL policy for outbound traffic.
ports	Array of strings	Specifies the list of ports bound with the network ACL group.
public	Boolean	Specifies whether the firewall group can be shared by different tenants.

Attribute	Type	Description
status	String	Specifies the status of the network ACL policy. The value can be: • **ACTIVE** (Normal) • **INACTIVE** (Inactive) • **ERROR** (Error occurred) • **PENDING_CREATE** (Creating) • **PENDING_UPDATE** (Updating) • **PENDING_DELETE** (Deleting)
admin_state_up	Boolean	Specifies the administrative status of the network ACL.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the resource is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "firewall_group": {
        "status": "PENDING_CREATE",
        "public": false,
        "egress_firewall_policy_id": null,
        "name": "test",
        "admin_state_up": true,
        "ports": [
            "c133f2bf-6937-4416-bb17-012e1be5cd2d"
        ],
        "tenant_id": "23c8a121505047b6869edf39f3062712",
        "id": "0415f554-26ed-44e7-a881-bdf4e6216e38",
        "ingress_firewall_policy_id": "afc52ce9-5305-4ec9-9feb-44feb8330341",
        "description": "",
        "project_id": "23c8a121505047b6869edf39f3062712",
        "created_at": "2018-09-12T08:24:14",
        "updated_at": "2018-09-12T08:24:14"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.16 Updating a Network ACL Group

Function

This API is used to update a network ACL group.

URI

PUT /v2.0/fwaas/firewall_groups/{firewall_group_id}

Request Parameters

Table 6-169 Request parameter

Parameter	Type	Mandatory	Description
firewall_group	**firewall_group** object	Yes	Specifies the firewall group. For details, see **Table 6-170**.

Table 6-170 Firewall Group objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the name of the network ACL group. The value can contain a maximum of 255 characters.
description	No	String	Provides supplementary information about the network ACL group. The value can contain a maximum of 255 characters.
ingress_firewall_policy_id	No	String	Specifies the network ACL policy for inbound traffic.
egress_firewall_policy_id	No	String	Specifies the network ACL policy for outbound traffic.

Attribute	Mandatory	Type	Description
ports	No	Array of strings	Specifies the list of ports bound with the network ACL group. The value must be the port ID. **NOTE** The port is the one whose **device_owner** is **network:router_interface_distributed**. • Call the VPC API for querying the port ID. For details, see **Querying Ports**. The filtering criteria are the specified **network_id** and **device_owner**. The **network_id** is the network ID of the subnet associated with the network ACL. Example: GET https://{Endpoint}/v1/{project_id}/ports?network_id={network_id}&device_owner=network%3Arouter_interface_distributed
admin_state_up	No	Boolean	Specifies the administrative status of the network ACL. The value can be **true** or **false**.

Example Request

Associate the ACL group whose ID is 2fb0e81f-9f63-44b2-9894-c13a3284594a with the outbound ACL policy 53f36c32-db25-4856-a0ba-e605fd88c5e9.

```
PUT https://{Endpoint}/v2.0/fwaas/firewall_groups/2fb0e81f-9f63-44b2-9894-c13a3284594a

{
    "firewall_group": {
        "egress_firewall_policy_id": "53f36c32-db25-4856-a0ba-e605fd88c5e9"
    }
}
```

Response Parameters

Table 6-171 Response parameter

Parameter	Type	Description
firewall_group	**firewall_group** object	Specifies the firewall group. For details, see **Table 6-172**.

Table 6-172 Firewall Group objects

Attribute	Type	Description
id	String	Specifies the UUID of the network ACL group.
name	String	Specifies the name of the network ACL group.
description	String	Provides supplementary information about the network ACL group.
tenant_id	String	Specifies the project ID.
ingress_firewall_policy_id	String	Specifies the network ACL policy for inbound traffic.
egress_firewall_policy_id	String	Specifies the network ACL policy for outbound traffic.
ports	Array of strings	Specifies the list of ports bound with the network ACL group.
public	Boolean	Specifies whether the firewall group can be shared by different tenants.
status	String	Specifies the status of the network ACL policy. The value can be: • **ACTIVE** (Normal) • **INACTIVE** (Inactive) • **ERROR** (Error occurred) • **PENDING_CREATE** (Creating) • **PENDING_UPDATE** (Updating) • **PENDING_DELETE** (Deleting)
admin_state_up	Boolean	Specifies the administrative status of the network ACL.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the resource is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the resource is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "firewall_group": {
        "status": "PENDING_UPDATE",
        "public": false,
        "egress_firewall_policy_id": "53f36c32-db25-4856-a0ba-e605fd88c5e9",
        "name": "",
        "admin_state_up": true,
        "ports": [
            "c133f2bf-6937-4416-bb17-012e1be5cd2d"
        ],
        "tenant_id": "23c8a121505047b6869edf39f3062712",
        "id": "0415f554-26ed-44e7-a881-bdf4e6216e38",
        "ingress_firewall_policy_id": "afc52ce9-5305-4ec9-9feb-44feb8330341",
        "description": "",
        "project_id": "23c8a121505047b6869edf39f3062712",
        "created_at": "2018-09-12T08:24:14",
        "updated_at": "2018-09-12T08:24:14"
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.6.17 Deleting a Network ACL Group

Function

This API is used to delete a network ACL group.

URI

DELETE /v2.0/fwaas/firewall_groups/{firewall_group_id}

Table 6-173 describes the parameters.

Table 6-173 Parameter description

Parameter	Mandatory	Type	Description
firewall_group_id	Yes	String	Specifies the network ACL group ID, which uniquely identifies the network ACL group.

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/fwaas/firewall_groups/0415f554-26ed-44e7-a881-bdf4e6216e38
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7 Security Group

6.7.1 Querying Security Groups

Function

This API is used to query all security groups accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/security-groups

Example of querying security groups by page

```
GET https://{Endpoint}/v2.0/security-groups?
limit=2&marker=0431c9c5-1660-42e0-8a00-134bec7f03e2&page_reverse=False
```

Table 6-174 describes the parameters.

Table 6-174 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the ID is used as the filtering condition.
name	No	String	Specifies that the name is used as the filtering condition.

Parameter	Mandatory	Type	Description
description	No	String	Specifies that the description is used as the filtering condition.
tenant_id	No	String	Specifies that the project ID is used as the filtering condition.
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. ● If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. ● If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. ● If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. ● If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/security-groups?limit=1
```

Response Parameters

Table 6-175 Response parameter

Parameter	Type	Description
security_groups	Array of **Security Group** objects	Specifies the security group list. For details, see **Table 6-176**.
security_groups_links	Array of **SecurityGroupsLink** objects	Shows pagination information about security groups. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-176 Security Group objects

Attribute	Type	Description
id	String	Specifies the security group ID. This parameter is not mandatory when you query security groups.
tenant_id	String	Specifies the project ID.
name	String	Specifies the security group name.
description	String	Provides supplementary information about the security group.
security_group_rules	Array of **Security Group Rule** objects	Specifies the security group rule list. For details, see **Table 6-177**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-177 Security Group Rule objects

Attribute	Type	Description
id	String	Specifies the security group rule ID. This parameter is not mandatory when you query security group rules.
description	String	Provides supplementary information about the security group rule.
security_group_id	String	Specifies the ID of the belonged security group.
remote_group_id	String	Specifies the peer ID of the belonged security group.
direction	String	Specifies the direction of the traffic for which the security group rule takes effect.
remote_ip_prefix	String	Specifies the peer IP address segment.
protocol	String	Specifies the protocol type or the IP protocol number.
port_range_max	Integer	Specifies the maximum port number. When ICMP is used, the value is the ICMP code.
port_range_min	Integer	Specifies the minimum port number. If the ICMP protocol is used, this parameter indicates the ICMP type. When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**).
ethertype	String	Specifies the network type. IPv4 and IPv6 are supported.
tenant_id	String	Specifies the project ID.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.

Attribute	Type	Description
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-178 SecurityGroupsLink objects

Parameter	Type	Description
href	String	Specifies the API link.
rel	String	Specifies the relationship between the API link and the API version.

Example Response


```
{
   "security_groups": [
      {
         "id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
         "name": "sg-ad3f",
         "description": "",
         "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
         "security_group_rules": [
            {
               "id": "d90e55ba-23bd-4d97-b722-8cb6fb485d69",
               "direction": "ingress",
               "protocol": null,
               "ethertype": "IPv4",
               "description": null,
               "remote_group_id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
               "remote_ip_prefix": null,
               "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
               "port_range_max": null,
               "port_range_min": null,
               "security_group_id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
               "remote_address_group_id": "0150a3a7-82ca-4569-865c-04e46e5e9249"
            },
            {
               "id": "aecff4d4-9ce9-489c-86a3-803aedec65f7",
               "direction": "egress",
               "protocol": null,
               "ethertype": "IPv4",
               "description": null,
               "remote_group_id": null,
               "remote_ip_prefix": null,
               "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
               "port_range_max": null,
```



```
                "port_range_min": null,
                "security_group_id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
                "remote_address_group_id": null
            }
        ],
        "created_at": "2018-09-12T08:24:14",
        "updated_at": "2018-09-12T08:24:14"
    }
  ],
  "security_groups_links": [
    {
        "rel": "next",
        "href": "https://{Endpoint}/v2.0/security-groups?
limit=1&marker=0431c9c5-1660-42e0-8a00-134bec7f03e2"
    },
    {    "rel": "previous",
        "href": "https://{Endpoint}/v2.0/security-groups?
limit=1&marker=0431c9c5-1660-42e0-8a00-134bec7f03e2&page_reverse=True"
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.2 Querying a Security Group

Function

This API is used to query details about a specific security group.

URI

GET /v2.0/security-groups/{security_group_id}

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/security-groups/0431c9c5-1660-42e0-8a00-134bec7f03e2
```

Response Parameters

Table 6-179 Response parameter

Parameter	Type	Description
security_group	**security_group** object	Specifies the security group. For details, see **Table 6-180**.

Table 6-180 Security Group objects

Attribute	Type	Description
id	String	Specifies the security group ID. This parameter is not mandatory when you query security groups.
tenant_id	String	Specifies the project ID.
name	String	Specifies the security group name.
description	String	Provides supplementary information about the security group.
security_group_rules	Array of **Security Group Rule** objects	Specifies the security group rule list. For details, see **Table 6-181**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-181 Security Group Rule objects

Attribute	Type	Description
id	String	Specifies the security group rule ID. This parameter is not mandatory when you query security group rules.
description	String	Provides supplementary information about the security group rule.
security_group_id	String	Specifies the ID of the belonged security group.
remote_group_id	String	Specifies the peer ID of the belonged security group.
direction	String	Specifies the direction of the traffic for which the security group rule takes effect.
remote_ip_prefix	String	Specifies the peer IP address segment.

Attribute	Type	Description
protocol	String	Specifies the protocol type or the IP protocol number.
port_range_max	Integer	Specifies the maximum port number. When ICMP is used, the value is the ICMP code.
port_range_min	Integer	Specifies the minimum port number. If the ICMP protocol is used, this parameter indicates the ICMP type. When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**).
ethertype	String	Specifies the network type. IPv4 and IPv6 are supported.
tenant_id	String	Specifies the project ID.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "security_group": {
        "id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
        "name": "sg-ad3f",
```



```
    "description": "",
    "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "security_group_rules": [
      {
        "id": "d90e55ba-23bd-4d97-b722-8cb6fb485d69",
        "direction": "ingress",
        "protocol": null,
        "ethertype": "IPv4",
        "description": null,
        "remote_group_id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
        "remote_ip_prefix": null,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "port_range_max": null,
        "port_range_min": null,
        "security_group_id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
        "remote_address_group_id": "0150a3a7-82ca-4569-865c-04e46e5e9249"
      },
      {
        "id": "aecff4d4-9ce9-489c-86a3-803aedec65f7",
        "direction": "egress",
        "protocol": null,
        "ethertype": "IPv4",
        "description": null,
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "port_range_max": null,
        "port_range_min": null,
        "security_group_id": "0431c9c5-1660-42e0-8a00-134bec7f03e2",
        "remote_address_group_id": null
      }
    ],
    "created_at": "2018-09-12T08:24:14",
    "updated_at": "2018-09-12T08:24:14"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.3 Creating a Security Group

Function

This API is used to create a security group.

URI

POST /v2.0/security-groups

Request Parameters

Table 6-182 Request parameter

Parameter	Mandatory	Type	Description
security_group	Yes	**security_group** object	Specifies the security group. For details, see **Table 6-183**.

Table 6-183 Security Group objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the security group name.
description	No	String	Provides supplementary information about the security group.

Example Request

Create a security group named **sg-test**.

```
POST https://{Endpoint}/v2.0/security-groups

{
    "security_group": {
        "name": "sg-test"
    }
}
```

Response Parameters

Table 6-184 Response parameter

Parameter	Type	Description
security_group	**security_group** object	Specifies the security group. For details, see **Table 6-185**.

Table 6-185 Security Group objects

Attribute	Type	Description
id	String	Specifies the security group ID. This parameter is not mandatory when you query security groups.
tenant_id	String	Specifies the project ID.
name	String	Specifies the security group name.
description	String	Provides supplementary information about the security group.
security_group_rules	Array of **Security Group Rule** objects	Specifies the security group rule list. For details, see **Table 6-186**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-186 Security Group Rule objects

Attribute	Type	Description
id	String	Specifies the security group rule ID. This parameter is not mandatory when you query security group rules.
description	String	Provides supplementary information about the security group rule.
security_group_id	String	Specifies the ID of the belonged security group.
remote_group_id	String	Specifies the peer ID of the belonged security group.
direction	String	Specifies the direction of the traffic for which the security group rule takes effect.
remote_ip_prefix	String	Specifies the peer IP address segment.

Attribute	Type	Description
protocol	String	Specifies the protocol type or the IP protocol number.
port_range_max	Integer	Specifies the maximum port number. When ICMP is used, the value is the ICMP code.
port_range_min	Integer	Specifies the minimum port number. If the ICMP protocol is used, this parameter indicates the ICMP type. When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**).
ethertype	String	Specifies the network type. IPv4 and IPv6 are supported.
tenant_id	String	Specifies the project ID.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "security_group": {
        "id": "d29ae17d-f355-4992-8747-1fb66cc9afd2",
        "name": "sg-test",
```



```
    "description": "",
    "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "security_group_rules": [
      {
        "id": "3f51e52c-0e85-40f7-a137-85927392e436",
        "direction": "egress",
        "protocol": null,
        "ethertype": "IPv4",
        "description": null,
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "port_range_max": null,
        "port_range_min": null,
        "security_group_id": "d29ae17d-f355-4992-8747-1fb66cc9afd2",
        "remote_address_group_id": null
      },
      {
        "id": "6332de3e-98fb-4f8c-b44a-fcb8ff09881e",
        "direction": "egress",
        "protocol": null,
        "ethertype": "IPv6",
        "description": null,
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "port_range_max": null,
        "port_range_min": null,
        "security_group_id": "d29ae17d-f355-4992-8747-1fb66cc9afd2",
        "remote_address_group_id": null
      }
    ],
    "created_at": "2018-09-20T02:15:34",
    "updated_at": "2018-09-20T02:15:34"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.4 Updating a Security Group

Function

This API is used to update a security group.

URI

PUT /v2.0/security-groups/{security_group_id}

Request Parameters

Table 6-187 Request parameter

Parameter	Type	Mandatory	Description
security_group	**security_group** object	Yes	Specifies the security group. For details, see **Table 6-188**. You must specify at least one attribute when updating a security group.

Table 6-188 Security Group objects

Attribute	Mandatory	Type	Description
name	No	String	Specifies the security group name.
description	No	String	Provides supplementary information about the security group.

Example Request

Change the name of the security group whose ID is d29ae17d-f355-4992-8747-1fb66cc9afd2 to **sg-test02**.

```
PUT https://{Endpoint}/v2.0/security-groups/d29ae17d-f355-4992-8747-1fb66cc9afd2

{
   "security_group": {
         "name": "sg-test02"
   }
}
```

Response Parameters

Table 6-189 Response parameter

Parameter	Type	Description
security_group	**security_group** object	Specifies the security group objects. For details, see **Table 6-190**.

Table 6-190 Security Group objects

Attribute	Type	Description
id	String	Specifies the security group ID. This parameter is not mandatory when you query security groups.
tenant_id	String	Specifies the project ID.
name	String	Specifies the security group name.
description	String	Provides supplementary information about the security group.
security_group_rules	Array of **Security Group Rule** objects	Specifies the security group rule list. For details, see **Table 6-191**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-191 Security Group Rule objects

Attribute	Type	Description
id	String	Specifies the security group rule ID. This parameter is not mandatory when you query security group rules.
description	String	Provides supplementary information about the security group rule.
security_group_id	String	Specifies the ID of the belonged security group.
remote_group_id	String	Specifies the peer ID of the belonged security group.
direction	String	Specifies the direction of the traffic for which the security group rule takes effect.
remote_ip_prefix	String	Specifies the peer IP address segment.

Attribute	Type	Description
protocol	String	Specifies the protocol type or the IP protocol number.
port_range_max	Integer	Specifies the maximum port number. When ICMP is used, the value is the ICMP code.
port_range_min	Integer	Specifies the minimum port number. If the ICMP protocol is used, this parameter indicates the ICMP type. When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**).
ethertype	String	Specifies the network type. IPv4 and IPv6 are supported.
tenant_id	String	Specifies the project ID.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "security_group": {
        "id": "d29ae17d-f355-4992-8747-1fb66cc9afd2",
        "name": "sg-test02",
```



```
    "description": "",
    "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "project_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
    "security_group_rules": [
      {
        "id": "6332de3e-98fb-4f8c-b44a-fcb8ff09881e",
        "direction": "egress",
        "protocol": null,
        "ethertype": "IPv6",
        "description": null,
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "port_range_max": null,
        "port_range_min": null,
        "security_group_id": "d29ae17d-f355-4992-8747-1fb66cc9afd2",
        "remote_address_group_id": "0150a3a7-82ca-4569-865c-04e46e5e9249"
      },
      {
        "id": "3f51e52c-0e85-40f7-a137-85927392e436",
        "direction": "egress",
        "protocol": null,
        "ethertype": "IPv4",
        "description": null,
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "tenant_id": "bbfe8c41dd034a07bebd592bf03b4b0c",
        "port_range_max": null,
        "port_range_min": null,
        "security_group_id": "d29ae17d-f355-4992-8747-1fb66cc9afd2",
        "remote_address_group_id": null
      }
    ],
    "created_at": "2018-09-20T02:15:34",
    "updated_at": "2018-09-20T02:16:31"
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.5 Deleting a Security Group

Function

This API is used to delete a security group.

URI

DELETE /v2.0/security-groups/{security_group_id}

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/security-groups/a7ebb1d8-71e5-42e5-9030-4e0fca059d50
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.6 Querying Security Group Rules

Function

This API is used to query all security group rules accessible to the tenant submitting the request. A maximum of 2000 records can be returned for each query operation. If the number of records exceeds 2000, the pagination marker will be returned. For details, see section **Pagination**.

URI

GET /v2.0/security-group-rules

Example:

```
GET https://{Endpoint}/v2.0/security-group-rules?
security_group_id={security_group_id}&remote_group_id={remote_group_id}&direction={direction}&remote_ip_prefix={remote_ip_prefix}&protocol={protocol}&port_range_max={port_range_max}&port_range_min={port_range_min}&ethertype={ethertype}&tenant_id ={tenant_id}
```

Example of querying security group rules by page

```
GET https://{Endpoint}/v2.0/networks?limit=2&marker=07adc044-3f21-4eeb-bd57-5e5eb6024b7f&page_reverse=False
```

Table 6-192 describes the parameters.

Table 6-192 Parameter description

Parameter	Mandatory	Type	Description
id	No	String	Specifies that the security group rule ID is used as the filtering condition.

Parameter	Mandatory	Type	Description
description	No	String	Specifies that the description is used as the filtering condition.
remote_group_id	No	String	Specifies the ID of the remote security group associated with the security group rule is used as the filtering condition.
security_group_id	No	String	Specifies the ID of the corresponding security group is used as the filtering condition.
direction	No	String	Specifies the security group rule direction is used as the filtering condition. The value can be **ingress** or **egress**.
protocol	No	String	Specifies that the IP protocol is used as the filtering condition.
remote_ip_prefix	No	String	Specifies the remote IP address range matching the security group rule is used as the filtering condition.
ethertype	No	String	Specifies that the network type is used as the filtering condition.
port_range_max	No	Integer	Specifies that the maximum port is used as the filtering condition.
port_range_min	No	Integer	Specifies that the minimum port is used as the filtering condition.
tenant_id	No	String	Specifies that the project ID is used as the filtering condition.

Parameter	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/security-group-rules
```

Response Parameters

Table 6-193 Response parameter

Parameter	Type	Description
security_group_rules	Array of **Security Group Rule** objects	Specifies the security group rule list. For details, see **Table 6-194**.
security_group_rules_links	Array of **SecurityGroupRulesLink** objects	Shows pagination information about security group rules. Only when **limit** is used for filtering and the number of resources exceeds the value of **limit** or 2000 (default value of **limit**), value **next** will be returned for **rel** and a link for **href**.

Table 6-194 Security Group Rule objects

Attribute	Type	Description
id	String	Specifies the security group rule ID. This parameter is not mandatory when you query security group rules.
description	String	Provides supplementary information about the security group rule.
security_group_id	String	Specifies the ID of the belonged security group.
remote_group_id	String	Specifies the peer ID of the belonged security group.
direction	String	Specifies the direction of the traffic for which the security group rule takes effect.
remote_ip_prefix	String	Specifies the peer IP address segment.
protocol	String	Specifies the protocol type or the IP protocol number.

Attribute	Type	Description
port_range_max	Integer	Specifies the maximum port number. When ICMP is used, the value is the ICMP code.
port_range_min	Integer	Specifies the minimum port number. If the ICMP protocol is used, this parameter indicates the ICMP type. When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**).
ethertype	String	Specifies the network type. IPv4 and IPv6 are supported.
tenant_id	String	Specifies the project ID.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: *yyyy-MM-ddTHH:mm:ss*
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Table 6-195 SecurityGroupRulesLink objects

Parameter	Type	Description
href	String	Specifies the API link.

Parameter	Type	Description
rel	String	Specifies the relationship between the API link and the API version.

Example Response


```
{
   "security_group_rules": [
      {
         "remote_group_id": "1d8b19c7-7c56-48f7-a99b-4b40eb390967",
         "direction": "ingress",
         "remote_ip_prefix": null,
         "protocol": null,
         "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
         "port_range_max": null,
         "security_group_id": "1d8b19c7-7c56-48f7-a99b-4b40eb390967",
         "port_range_min": null,
         "ethertype": "IPv6",
         "description": null,
         "id": "07adc044-3f21-4eeb-bd57-5e5eb6024b7f",
         "project_id": "6c9298ec8c874f7f99688489ab65f90e",
         "created_at": "2018-09-20T02:15:34",
         "updated_at": "2018-09-20T02:15:34",
         "remote_address_group_id": null
      },
      {
         "remote_group_id": null,
         "direction": "egress",
         "remote_ip_prefix": null,
         "protocol": null,
         "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
         "port_range_max": null,
         "security_group_id": "328fb454-a2ee-4a11-bdb1-ee19bbdfde43",
         "port_range_min": null,
         "ethertype": "IPv6",
         "description": null,
         "id": "09358f83-f4a5-4386-9563-a1e3c373d655",
         "project_id": "6c9298ec8c874f7f99688489ab65f90e",
         "created_at": "2018-09-20T02:15:34",
         "updated_at": "2018-09-20T02:15:34",
         "remote_address_group_id": null
      },
      {
         "remote_group_id": "4c763030-366e-428c-be2b-d48f6baf5297",
         "direction": "ingress",
         "remote_ip_prefix": null,
         "protocol": null,
         "tenant_id": "6c9298ec8c874f7f99688489ab65f90e",
         "port_range_max": null,
         "security_group_id": "4c763030-366e-428c-be2b-d48f6baf5297",
         "port_range_min": null,
         "ethertype": "IPv6",
         "description": null,
         "id": "219a6f56-1069-458b-bec0-df9270e7a074",
         "project_id": "6c9298ec8c874f7f99688489ab65f90e",
         "created_at": "2018-09-20T02:15:34",
         "updated_at": "2018-09-20T02:15:34",
         "remote_address_group_id": null
      }
   ],
   "security_group_rules_links": [
     {    "rel": "previous",
         "href": "https://{Endpoint}/v2.0/
security-group-rules?marker=07adc044-3f21-4eeb-bd57-5e5eb6024b7f&page_reverse=True"
      }
```



```
  ]
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.7 Querying a Security Group Rule

Function

This API is used to query details about a specific security group rule.

URI

GET /v2.0/security-group-rules/{security_group_rule_id}

Request Parameters

None

Example Request

```
GET https://{Endpoint}/v2.0/security-group-rules/1755bc80-cf3a-4f57-8ae9-d9796482ddc0
```

Response Parameters

Table 6-196 Response parameter

Parameter	Type	Description
security_group_rule	**security_group_rule** object	Specifies the security group rule. For details, see **Table 6-197**.

Table 6-197 Security Group Rule objects

Attribute	Type	Description
id	String	Specifies the security group rule ID. This parameter is not mandatory when you query security group rules.
description	String	Provides supplementary information about the security group rule.

Attribute	Type	Description
security_group_id	String	Specifies the ID of the belonged security group.
remote_group_id	String	Specifies the peer ID of the belonged security group.
direction	String	Specifies the direction of the traffic for which the security group rule takes effect.
remote_ip_prefix	String	Specifies the peer IP address segment.
protocol	String	Specifies the protocol type or the IP protocol number.
port_range_max	Integer	Specifies the maximum port number. When ICMP is used, the value is the ICMP code.
port_range_min	Integer	Specifies the minimum port number. If the ICMP protocol is used, this parameter indicates the ICMP type. When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**).
ethertype	String	Specifies the network type. IPv4 and IPv6 are supported.
tenant_id	String	Specifies the project ID.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	Specifies the time (UTC) when the security group rule is created. Format: *yyyy-MM-ddTHH:mm:ss*

Attribute	Type	Description
updated_at	String	Specifies the time (UTC) when the security group rule is updated. Format: *yyyy-MM-ddTHH:mm:ss*

Example Response

```
{
    "security_group_rule": {
        "remote_group_id": null,
        "direction": "egress",
        "remote_ip_prefix": null,
        "protocol": null,
        "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
        "port_range_max": null,
        "security_group_id": "723bc02c-d7f7-49b5-b6ff-d08320f315e2",
        "port_range_min": null,
        "ethertype": "IPv4",
        "description": null,
        "id": "1755bc80-cf3a-4f57-8ae9-d9796482ddc0",
        "project_id": "6fbe9263116a4b68818cf1edce16bc4f",
        "created_at": "2018-09-20T02:15:34",
        "updated_at": "2018-09-20T02:15:34",
        "remote_address_group_id": null
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.8 Creating a Security Group Rule

Function

This API is used to create a security group rule.

URI

POST /v2.0/security-group-rules

Request Parameters

Table 6-198 Request parameter

Parameter	Type	Mandatory	Description
security_group_rule	**security_group_rule** object	Yes	Specifies the security group rule. For details, see **Table 6-199**.

Table 6-199 Security Group Rule objects

Attribute	Mandatory	Type	Description
description	No	String	Provides supplementary information about the security group rule.
security_group_id	Yes	String	Specifies the ID of the belonged security group.
remote_group_id	No	String	• Specifies the peer ID of the belonged security group. • This parameter is mutually exclusive with **remote_ip_prefix** and **remote_address_group_id**.
direction	Yes	String	• Specifies the direction of a security group rule. • The value can be **ingress** (inbound) or **egress** (outbound).
remote_ip_prefix	No	String	• Specifies the peer IP address segment. • This parameter is mutually exclusive with **remote_group_id** and **remote_address_group_id**.
protocol	No	String	• Specifies the protocol type or the IP protocol number. • The value can be **tcp**, **udp**, **icmp** or an IP protocol number.

Attribute	Mandatory	Type	Description
port_range_max	No	Integer	• Specifies the maximum port number. When ICMP is used, the value is the ICMP code. • The value ranges from 1 to 65535. (The value ranges from 0 to 255 when it indicates the code.)
port_range_min	No	Integer	• Specifies the minimum port number. When ICMP is used, the value is the ICMP type. • Constraints: – When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. – When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**). • The value ranges from 1 to 65535. (The value ranges from 0 to 255 when it indicates the code.)
ethertype	No	String	• Specifies the network type. • The value can be **IPv4** or **IPv6**.
remote_address_group_id	No	String	• Specifies the remote IP address group ID. You can log in to the management console and view the ID on the IP address group page. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.

Example Request

Create an outbound rule in the security group whose ID is 5cb9c1ee-00e0-4d0f-9623-55463cd26ff8. Set **protocol** to **tcp**, and **remote_ip_prefix** to 10.10.0.0/24.

```
POST https://{Endpoint}/v2.0/security-group-rules

{
   "security_group_rule": {
      "security_group_id": "5cb9c1ee-00e0-4d0f-9623-55463cd26ff8",
      "direction": "egress",
      "protocol": "tcp",
      "remote_ip_prefix": "10.10.0.0/24"
   }
}
```

Response Parameters

Table 6-200 Response parameter

Parameter	Type	Description
security_group_rule	**security_group_rule** object	Specifies the security group rule. For details, see **Table 6-201**.

Table 6-201 Security Group Rule objects

Attribute	Type	Description
id	String	• Specifies the security group rule ID. • This parameter is not mandatory when you query security group rules.
description	String	Provides supplementary information about the security group rule.
security_group_id	String	Specifies the ID of the belonged security group.
remote_group_id	String	Specifies the peer ID of the belonged security group.
direction	String	Specifies the direction of a security group rule.
remote_ip_prefix	String	Specifies the peer IP address segment.
protocol	String	Specifies the protocol type or the IP protocol number.

Attribute	Type	Description
port_range_max	Integer	• Specifies the maximum port number. When ICMP is used, the value is the ICMP code. • The value ranges from 1 to 65535. (The value ranges from 0 to 255 when it indicates the code.)
port_range_min	Integer	• Specifies the minimum port number. When ICMP is used, the value is the ICMP type. • Constraints: – When the TCP or UDP protocol is used, both **port_range_max** and **port_range_min** must be specified, and the **port_range_max** value must be greater than the **port_range_min** value. – When the ICMP protocol is used, if you specify the ICMP code (**port_range_max**), you must also specify the ICMP type (**port_range_min**).
ethertype	String	• Specifies the IP version. • The value can be **IPv4** or **IPv6**.
tenant_id	String	Specifies the project ID.
remote_address_group_id	String	• Specifies the remote IP address group ID. • The value is mutually exclusive with parameters **remote_ip_prefix** and **remote_group_id**.
project_id	String	Specifies the project ID. For details about how to obtain a project ID, see **Obtaining a Project ID**.
created_at	String	• Time when the security group rule is created • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ
updated_at	String	• Time when the security group rule is updated • UTC time in the format of yyyy-MM-ddTHH:mm:ssZ

Example Response


```
{
   "security_group_rule": {
      "remote_group_id": null,
      "direction": "egress",
      "remote_ip_prefix": "10.10.0.0/24",
      "protocol": "tcp",
      "tenant_id": "6fbe9263116a4b68818cf1edce16bc4f",
      "port_range_max": null,
      "security_group_id": "5cb9c1ee-00e0-4d0f-9623-55463cd26ff8",
      "port_range_min": null,
      "ethertype": "IPv4",
      "description": null,
      "id": "7c336b04-1603-4911-a6f4-f2af1d9a0488",
      "project_id": "6fbe9263116a4b68818cf1edce16bc4f",
      "created_at": "2018-09-20T02:15:34",
      "updated_at": "2018-09-20T02:15:34",
      "remote_address_group_id": null
   }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

6.7.9 Deleting a Security Group Rule

Function

This API is used to delete a security group rule.

URI

DELETE /v2.0/security-group-rules/{security_group_rule_id}

Request Parameters

None

Response Parameters

None

Example Request

```
DELETE https://{Endpoint}/v2.0/security-group-rules/07adc044-3f21-4eeb-bd57-5e5eb6024b7f
```

Example Response

None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

7 Application Examples

7.1 Example 1: Creating a VPC and Subnet for an ECS

Scenarios

This section describes how to create a VPC and subnet for an ECS by calling APIs.

Prerequisites

You have planned the region where you want to create the VPC and obtained the endpoint required for calling APIs. For details, see **Endpoints**.

If you use a token for authentication, you must obtain the token and add **X-Auth-Token** to the request header when making an API call. Obtain the token by referring to **Authentication**.

NOTE

The token obtained from IAM is valid for only 24 hours. If you want to use a token for authentication, you can cache it to avoid frequent calling.

Procedure

1. Create a VPC.
   a. Send **POST https://*VPC endpoint*/v1/{project_id}/vpcs**. Parameter **project_id** indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Set the following parameters in the request body. Plan the value of the **cidr** field in advance.

```
{
   "vpc": {
      "name": "vpc", //VPC name
      "cidr": "192.168.0.0/16" //Available subnet in the VPC
   }
}
```

   d. Check the response message.

- The request is successful if the following response is displayed. In the response, **id** indicates the VPC ID.

```
{
   "vpc": {
      "id": "b6684a27-b049-407d-90b4-c9551f2390e1",
      "name": "vpc",
      "cidr": "192.168.0.0/16",
      "status": "CREATING",
      "routes": []
   }
}
```

- For details about the error codes displayed if the request fails, see section **Error Codes**.

2. View details of the VPC.
   a. Send **GET https://*VPC endpoint*/v1/{project_id}/vpcs/{vpc_id}**. Parameter **project_id** indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Check the response message.

- The request is successful if the following response is displayed. In the response, **id** indicates the VPC ID.

```
{
   "vpc": {
      "id": "b6684a27-b049-407d-90b4-c9551f2390e1",
      "name": "vpc",
      "description": "",
      "cidr": "192.168.0.0/16",
      "status": "OK",
      "enterprise_project_id": "0" ,
      "routes": []
   }
}
```

- For details about the error codes displayed if the request fails, see section **Error Codes**.

3. Create a subnet in the VPC.
   a. Send **POST https://*VPC endpoint*/v1/{project_id}/subnets**. Parameter **project_id** indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Set the following parameters in the request body. For details about the values of **dnsList**, see **What Are the Private DNS Server Addresses Provided by the DNS Service?** For details about the values of **availability_zone**, see **Regions and Endpoints**.
   d.

```
{
   "subnet": {
      "name": "subnet",
      "description": "",
      "cidr": "192.168.0.0/24",
      "gateway_ip": "192.168.0.1",
      "dhcp_enable": true,
      "dnsList": ["114.xx.xx.114", "114.xx.xx.115"],
      "availability_zone": "aa-bb-cc",
      "vpc_id": "b6684a27-b049-407d-90b4-c9551f2390e1"
   }
}
```

   e. Check the response message.

- The request is successful if the following response is displayed.

```
{
   "subnet": {
      "id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "name": "subnet",
      "description": "",
      "cidr": "192.168.0.0/24",
      "dnsList": ["114.xx.xx.114", "1114.xx.xx.115"],
      "status": "UNKNOWN",
      "vpc_id": "b6684a27-b049-407d-90b4-c9551f2390e1",
      "gateway_ip": "192.168.0.1",
      "dhcp_enable": true,
      "primary_dns": "114.xx.xx.114",
      "secondary_dns": "114.xx.xx.115",
      "availability_zone": "aa-bb-cc",
      "neutron_network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "neutron_subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
      "extra_dhcp_opts": []
   }
}
```

- For details about the error codes displayed if the request fails, see section **Error Codes**.

4. View details of the subnet.
   a. Send **GET https://*VPC endpoint*/v1/{project_id}/subnets/{subnet_id}**. Parameter **project_id** indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Check the response message.

```
{
   "subnet": {
      "id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "name": "subnet",
      "description": "",
      "cidr": "192.168.20.0/24",
      "dnsList": ["114.xx.xx.114", "114.xx.xx.115"],
      "status": "ACTIVE",
      "vpc_id": "b6684a27-b049-407d-90b4-c9551f2390e1",
      "gateway_ip": "192.168.20.1",
      "ipv6_enable": false,
      "dhcp_enable": true,
      "primary_dns": "114.xx.xx.114",
      "secondary_dns": "114.xx.xx.115",
      "availability_zone": "aa-bb-cc",
      "neutron_network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "neutron_subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
      "extra_dhcp_opts": []
   }
}
```

7.2 Example 2: Configuring a Security Group for an ECS

Scenarios

This section describes how to configure a security group for an ECS by calling APIs.

Prerequisites

- You have purchased an ECS. For details, see **Overview**.

- If you use a token for authentication, you must obtain the token and add **X-Auth-Token** to the request header when making an API call. Obtain the token by referring to **Authentication**.

NOTE

The token obtained from IAM is valid for only 24 hours. If you want to use a token for authentication, you can cache it to avoid frequent calling.

Procedure

1. Obtain the NIC information based on the ECS ID.
   a. Send **GET https://*VPC endpoint*/v1/{project_id}/ports?device_id={ecs_id}**. Parameter **project_id** indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Check the response message.
      - The request is successful if the following response is displayed.

```
{
   "ports": [{
      "id": "02c72193-efec-42fb-853b-c33f2b802467",
      "name": "",
      "status": "ACTIVE",
      "admin_state_up": true,
      "fixed_ips": [{
         "subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
         "ip_address": "192.168.0.75"
      }],
      "mac_address": "fa:16:3e:47:5f:c1",
      "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
      "project_id": "db82c9e1415a464ea68048baa8acc6b8",
      "device_id": "ea61f836-b52f-41bf-9d06-685644001d6f",
      "device_owner": "compute:br-iaas-odin1a",
      "security_groups": [
         "e0598d96-9451-4f8a-8de0-b8b4d451d9e7"
      ],
      "extra_dhcp_opts": [],
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "binding:vif_details": {
         "primary_interface": true
      },
      "binding:profile": {},
      "port_security_enabled": true,
      "created_at": "2020-06-20T08:07:29",
      "updated_at": "2020-06-20T08:07:29"
   }]
}
```

      - For details about the error codes displayed if the request fails, see section **Error Codes**.
2. View information about existing security groups.
   a. Send **GET https://*VPC endpoint*/v1/{project_id}/subnets/security-groups**. Parameter **project_id** indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Check the response message.
      - The request is successful if the following response is displayed. In the response, **id** indicates the security group ID.


```
{
   "security_groups": [{
      "id": "16b6e77a-08fa-42c7-aa8b-106c048884e6",
      "name": "qq",
      "description": "qq",
      "vpc_id": "3ec3b33f-ac1c-4630-ad1c-7dba1ed79d85",
      "enterprise_project_id ": "0aad99bc-f5f6-4f78-8404-c598d76b0ed2",
      "security_group_rules": [{
         "direction": "egress",
         "ethertype": "IPv4",
         "id": "369e6499-b2cb-4126-972a-97e589692c62",
         "description": "",
         "security_group_id": "16b6e77a-08fa-42c7-aa8b-106c048884e6"
      }, {
         "direction": "ingress",
         "ethertype": "IPv4",
         "id": "0222556c-6556-40ad-8aac-9fd5d3c06171",
         "description": "",
         "remote_group_id": "16b6e77a-08fa-42c7-aa8b-106c048884e6",
         "security_group_id": "16b6e77a-08fa-42c7-aa8b-106c048884e6"
      }]
   }, {
      "id": "9c0f56be-a9ac-438c-8c57-fce62de19419",
      "name": "default",
      "description": "qq",
      "vpc_id": "13551d6b-755d-4757-b956-536f674975c0",
      "enterprise_project_id ": "0",
      "security_group_rules": [{
         "direction": "egress",
         "ethertype": "IPv4",
         "id": "95479e0a-e312-4844-b53d-a5e4541b783f",
         "description": "",
         "security_group_id": "9c0f56be-a9ac-438c-8c57-fce62de19419"
      }, {
         "direction": "ingress",
         "ethertype": "IPv4",
         "id": "0c4a2336-b036-4fa2-bc3c-1a291ed4c431",
         "description": "",
         "remote_group_id": "9c0f56be-a9ac-438c-8c57-fce62de19419",
         "security_group_id": "9c0f56be-a9ac-438c-8c57-fce62de19419"
      }]
   }]
}
```


   - For details about the error codes displayed if the request fails, see section **Error Codes**.

3. Add the ECS to a security group.
   a. Send **PUT https://*VPC endpoint*/v1/{project_id}/ports/{port_id}**. Parameter **project_id** indicates the project ID.
   b. Add **X-Auth-Token** to the request header.
   c. Specify the following parameters in the request body:

```
{
   "port": {
      "security_groups": ["9c0f56be-a9ac-438c-8c57-fce62de19419","16b6e77a-08fa-42c7-aa8b-106c048884e6"]
   }
}
```

   d. Check the response message.
      - The request is successful if the following response is displayed. In the response, **id** indicates the port ID.


```
{
   "port": {
      "id": "02c72193-efec-42fb-853b-c33f2b802467",
      "name": "",
```



```
        "status": "ACTIVE",
        "admin_state_up": true,
        "fixed_ips": [{
            "subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
            "ip_address": "192.168.0.75"
        }],
        "mac_address": "fa:16:3e:47:5f:c1",
        "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
        "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
        "project_id": "db82c9e1415a464ea68048baa8acc6b8",
        "device_id": "ea61f836-b52f-41bf-9d06-685644001d6f",
        "device_owner": "compute:br-iaas-odin1a",
        "security_groups": ["9c0f56be-a9ac-438c-8c57-fce62de19419", "16b6e77a-08fa-42c7-
aa8b-106c048884e6"],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [{
            "ip_address": "1.1.1.1/0"
        }],
        "binding:vnic_type": "normal",
        "binding:vif_details": {
            "primary_interface": true
        },
        "binding:profile": {},
        "port_security_enabled": true,
        "created_at": "2020-06-20T08:07:29",
        "updated_at": "2020-06-20T08:07:29"
    }
}
```


- For details about the error codes displayed if the request fails, see section **Error Codes**.

7.3 Example 3: Assigning a Virtual IP Address to an ECS for HA

Scenarios

Virtual IP addresses are used for high availability as they make active/standby ECS switchover possible. This way if one ECS goes down for some reason, the other one can take over and services continue uninterrupted.

This section describes how to assign a virtual IP address to an ECS for HA by calling APIs.

Prerequisites

- You have created a VPC and subnet and obtained the VPC ID and subnet ID. For details, see **Creating a VPC and Subnet**.
- You have purchased an ECS. For details, see **Overview**.
- If you use a token for authentication, you must obtain the token and add **X-Auth-Token** to the request header when making an API call. Obtain the token by referring to **Authentication**.

NOTE

The token obtained from IAM is valid for only 24 hours. If you want to use a token for authentication, you can cache it to avoid frequent calling.

Procedure

1. Assign a virtual IP address.
   a. Send **POST https://*VPC endpoint*/v2.0/ports**.
   b. Add **X-Auth-Token** to the request header.
   c. Set the following parameters in the request body. The virtual IP address and the ECS must be in the same subnet.

```
{
   "port": {
      "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "device_owner": "neutron:VIP_PORT",
      "name": "vip_port_test"
   }
}
```

   Alternatively, you can assign a specific IP address.

```
{
   "port": {
      "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "device_owner": "neutron:VIP_PORT",
      "name": "vip_port_test",
      "fixed_ips": [
         {
            "ip_address": "192.168.0.220"
         }
      ]
   }
}
```

   d. Check the response message.
      - The request is successful if the following response is displayed.

```
{
   "port": {
      "id": "a7d98f3c-b42f-460b-96a1-07601e145961",
      "name": "port-test",
      "status": "DOWN",
      "admin_state_up": true,
      "fixed_ips": [{
         "subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
         "ip_address": "192.168.0.220"
      }],
      "mac_address": "fa:16:3e:01:f7:90",
      "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
      "project_id": "db82c9e1415a464ea68048baa8acc6b8",
      "device_id": "",
      "device_owner": "neutron:VIP_PORT",
      "security_groups": ["d0d58aa9-cda9-414c-9c52-6c3daf8534e6"],
      "extra_dhcp_opts": [],
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "binding:vif_details": {},
      "binding:profile": {},
      "port_security_enabled": true,
      "created_at": "2018-09-20T01:45:26",
      "updated_at": "2018-09-20T01:45:26"
   }
}
```

      - For details about the error codes displayed if the request fails, see section **Error Codes**.
2. Obtain the NIC information based on the ECS ID.
   a. Send **GET https://*VPC endpoint*/v2.0/ports?device_id={ecs_id}&network_id={network_id}**.

b. Add **X-Auth-Token** to the request header.

c. Check the response message.

- The request is successful if the following response is displayed.

```
{
   "ports": [{
      "id": "02c72193-efec-42fb-853b-c33f2b802467",
      "name": "",
      "status": "ACTIVE",
      "admin_state_up": true,
      "fixed_ips": [{
         "subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
         "ip_address": "192.168.0.75"
      }],
      "mac_address": "fa:16:3e:47:5f:c1",
      "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
      "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
      "project_id": "db82c9e1415a464ea68048baa8acc6b8",
      "device_id": "ea61f836-b52f-41bf-9d06-685644001d6f",
      "device_owner": "compute:br-iaas-odin1a",
      "security_groups": [
         "e0598d96-9451-4f8a-8de0-b8b4d451d9e7"
      ],
      "extra_dhcp_opts": [],
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "binding:vif_details": {
         "primary_interface": true
      },
      "binding:profile": {},
      "port_security_enabled": true,
      "created_at": "2020-06-20T08:07:29",
      "updated_at": "2020-06-20T08:07:29"
   }]
}
```

- For details about the error codes displayed if the request fails, see section **Error Codes**.

3. Bind an ECS to the virtual IP address.

a. Send **PUT https://***VPC endpoint***/v2.0/ports/***{port_id}*. *port_id* indicates the port ID corresponding to the assigned virtual IP address.

b. Add **X-Auth-Token** to the request header.

c. Set the following parameters in the request body. Set the value of **ip_address** to the NIC IP address of the ECS obtained in **2**.

```
{
   "port": {
      "allowed_address_pairs": [{
         "ip_address": "192.168.0.75"
      }]
   }
}
```

d. Check the response message.

- The request is successful if the following response is displayed.

```
{
   "port": {
      "id": "a7d98f3c-b42f-460b-96a1-07601e145961",
      "name": "port-test",
      "status": "DOWN",
      "admin_state_up": true,
      "fixed_ips": [{
         "subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
         "ip_address": "192.168.0.220"
      }],
```



```
        "mac_address": "fa:16:3e:01:f7:90",
        "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
        "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
        "project_id": "db82c9e1415a464ea68048baa8acc6b8",
        "device_id": "",
        "device_owner": "neutron:VIP_PORT",
        "security_groups": ["d0d58aa9-cda9-414c-9c52-6c3daf8534e6"],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [{
            "ip_address": "192.168.0.75"
        }]
        "binding:vnic_type": "normal",
        "binding:vif_details": {},
        "binding:profile": {},
        "port_security_enabled": true,
        "created_at": "2018-09-20T01:45:26",
        "updated_at": "2018-09-20T01:45:26"
    }
}
```


- For details about the error codes displayed if the request fails, see section **Error Codes**.

4. Disable the source/destination check function for the ECS NIC.
   a. Send **PUT https://***VPC endpoint***/v2.0/ports/***{port_id}*. **port_id** is the NIC ID obtained in **2**.
   b. Add **X-Auth-Token** to the request header.
   c. Set the following parameters in the request body. Set the value of **ip_address** to 1.1.1.1/0, the NIC IP address of the ECS.

```
{
    "port": {
        "allowed_address_pairs": [{
            "ip_address": "1.1.1.1/0"
        }]
    }
}
```

   d. Check the response message.
      - The request is successful if the following response is displayed.


```
{
    "port": {
        "id": "02c72193-efec-42fb-853b-c33f2b802467",
        "name": "",
        "status": "ACTIVE",
        "admin_state_up": true,
        "fixed_ips": [{
            "subnet_id": "213cb9d-3122-2ac1-1a29-91ffc1231a12",
            "ip_address": "192.168.0.75"
        }],
        "mac_address": "fa:16:3e:47:5f:c1",
        "network_id": "4779ab1c-7c1a-44b1-a02e-93dfc361b32d",
        "tenant_id": "db82c9e1415a464ea68048baa8acc6b8",
        "project_id": "db82c9e1415a464ea68048baa8acc6b8",
        "device_id": "ea61f836-b52f-41bf-9d06-685644001d6f",
        "device_owner": "compute:br-iaas-odin1a",
        "security_groups": ["e0598d96-9451-4f8a-8de0-b8b4d451d9e7"],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [{
            "ip_address": "1.1.1.1/0"
        }],
        "binding:vnic_type": "normal",
        "binding:vif_details": {
            "primary_interface": true
        },
        "binding:profile": {},
        "port_security_enabled": true,
```



```
        "created_at": "2020-06-20T08:07:29",
        "updated_at": "2020-06-20T08:07:29"
    }
}
```

- For details about the error codes displayed if the request fails, see section **Error Codes**.

7.4 Example 4: Assigning a Virtual IPv6 Address to ECSs for HA

Scenarios

Virtual IP addresses are used for high availability as they make active/standby ECS switchover possible. This way if one ECS goes down for some reason, the other one can take over and services continue uninterrupted.

This section describes how to assign a virtual IPv6 address to ECSs for HA by calling APIs.

Prerequisites

- You have created a VPC and a subnet that support both IPv4 and IPv6 and obtained the VPC ID and subnet ID. For details, see **Creating a VPC and Subnet**.
- You have purchased an ECS. For details, see **Overview**.
- If you use a token for authentication, you must obtain the token and add **X-Auth-Token** to the request header when making an API call. Obtain the token by referring to **Authentication**.

NOTE

The token obtained from IAM is valid for only 24 hours. If you want to use a token for authentication, you can cache it to avoid frequent calling.

Procedure

1. Assign a virtual IPv6 address.
   a. Send **POST https://***VPC endpoint***/v2.0/ports**.
   b. Add **X-Auth-Token** to the request header.
   c. Set the following parameters in the request body. The subnet where the virtual IP address resides must be the same as that of the ECS. Set **subnet_id** to the ID of the IPv6 subnet.

```
{
    "port":{
        "network_id":"b0ad9b80-bb16-4550-8ce0-514f949e35ee",
        "device_owner":"neutron:VIP_PORT",
        "name":"ipv6_vip_port_test",
        "fixed_ips":[
            {
                "subnet_id":"33ce2628-6246-4e3a-859f-99cd753ff704"
            }
        ]
    }
}
```


d. Check the response message.

- The request is successful if the following response is displayed:

```
{
   "port": {
      "id": "d92cfee7-9ebe-4483-85c1-00ffb1e45cd8",
      "name": "ipv6_vip_port_test",
      "status": "DOWN",
      "admin_state_up": true,
      "fixed_ips": [
         {
            "subnet_id": "33ce2628-6246-4e3a-859f-99cd753ff704",
            "ip_address": "2001:db8:a583:21d:2e25:9403:6f3d:4664"
         }
      ],
      "mac_address": "fa:16:3e:99:2e:92",
      "network_id": "b0ad9b80-bb16-4550-8ce0-514f949e35ee",
      "tenant_id": "060576782980d5762f9ec014dd2f1148",
      "project_id": "060576782980d5762f9ec014dd2f1148",
      "device_id": "",
      "device_owner": "neutron:VIP_PORT",
      "security_groups": [],
      "extra_dhcp_opts": [],
      "allowed_address_pairs": [],
      "binding:vnic_type": "normal",
      "binding:vif_details": {},
      "binding:profile": {},
      "port_security_enabled": true,
      "created_at": "2020-12-15T03:01:07",
      "updated_at": "2020-12-15T03:01:07"
   }
}
```

- For details about the error codes displayed if the request fails, see section **Error Codes**.

2. Query the NIC information according to the ECS ID. The value of **fixed_ips** contains IPv4 and IPv6 addresses.

   a. Send **GET https://***VPC endpoint***/v2.0/ports?device_id={ecs_id}&network_id={network_id}**.

   b. Add **X-Auth-Token** to the request header.

   c. Check the response message.

   - The request is successful if the following response is displayed:

```
{
    "ports": [{
        "id": "47b4cd46-cfe5-415d-957f-5068189dce94",
        "name": "",
        "status": "ACTIVE",
        "admin_state_up": true,
        "fixed_ips": [
           {
              "subnet_id": "0dd17989-1c23-4501-8dc1-40e4085f793f",
              "ip_address": "172.16.0.191"
           },
           {
              "subnet_id": "33ce2628-6246-4e3a-859f-99cd753ff704",
              "ip_address": "2001:db8:a583:21d:dfc0:d452:e9ab:65cf"
           }
        ],
        "mac_address": "fa:16:3e:1e:f7:9a",
        "network_id": "b0ad9b80-bb16-4550-8ce0-514f949e35ee",
        "tenant_id": "060576782980d5762f9ec014dd2f1148",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "device_id": "ab7ca781-66bf-48a8-814b-1568cb393a38",
        "device_owner": "compute:xxx",
```



```
        "security_groups": [
            "0552091e-b83a-49dd-88a7-4a5c86fd9ec3"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "binding:vif_details": {
            "primary_interface": true
        },
        "binding:profile": {},
        "port_security_enabled": true,
        "dns_assignment": [
            {
                "hostname": "ip-172-16-0-191",
                "ip_address": "172.16.0.191",
                "fqdn": "ip-172-16-0-191.br-iaas-odin1.compute.internal."
            }
        ],
        "dns_name": "ip-172-16-0-191",
        "created_at": "2020-11-19T13:32:37",
        "updated_at": "2020-11-19T13:33:50"
    }]
}
```


- For details about the error codes displayed if the request fails, see section **Error Codes**.

3. Bind an ECS to the virtual IP address.
   a. Send **PUT https://***VPC endpoint***/v2.0/ports/***{port_id}***.** *port_id* indicates the port ID corresponding to the assigned virtual IPv6 address.
   b. Add **X-Auth-Token** to the request header.
   c. Set the following parameters in the request body. Set the value of **ip_address** to the NIC IPv6 address of the ECS obtained in **2**.

```
{
    "port": {
        "allowed_address_pairs": [{
            "ip_address": "2001:db8:a583:21d:dfc0:d452:e9ab:65cf"
        }]
    }
}
```

   d. Check the response message.
      - The request is successful if the following response is displayed:


```
{
    "port": {
        "id": "d92cfee7-9ebe-4483-85c1-00ffb1e45cd8",
        "name": "ipv6_vip_port_test",
        "status": "DOWN",
        "admin_state_up": true,
        "fixed_ips": [
            {
                "subnet_id": "33ce2628-6246-4e3a-859f-99cd753ff704",
                "ip_address": "2001:db8:a583:21d:2e25:9403:6f3d:4664"
            }
        ],
        "mac_address": "fa:16:3e:99:2e:92",
        "network_id": "b0ad9b80-bb16-4550-8ce0-514f949e35ee",
        "tenant_id": "060576782980d5762f9ec014dd2f1148",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "device_id": "",
        "device_owner": "neutron:VIP_PORT",
        "security_groups": [],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [{
            "ip_address": "2001:db8:a583:21d:dfc0:d452:e9ab:65cf "
        }],
```



```
        "binding:vnic_type": "normal",
        "binding:vif_details": {},
        "binding:profile": {},
        "port_security_enabled": true,
        "created_at": "2020-12-15T03:01:07",
        "updated_at": "2020-12-15T03:01:07"
    }
}
```


- For details about the error codes displayed if the request fails, see section **Error Codes**.

4. Disable the source/destination check function for the ECS NIC.
   a. Send **PUT https://***VPC endpoint***/v2.0/ports/***{port_id}***. **port_id** is the NIC ID obtained in **2**.
   b. Add **X-Auth-Token** to the request header.
   c. Set the following parameters in the request body. Set the value of **ip_address** to 1.1.1.1/0, the NIC IP address of the ECS.

```
{
    "port": {
        "allowed_address_pairs": [{
            "ip_address": "1.1.1.1/0"
        }]
    }
}
```

   d. Check the response message.
      - The request is successful if the following response is displayed:


```
{
    "port": {
"id": "47b4cd46-cfe5-415d-957f-5068189dce94",
        "name": "",
        "status": "ACTIVE",
        "admin_state_up": true,
        "fixed_ips": [
            {
                "subnet_id": "0dd17989-1c23-4501-8dc1-40e4085f793f",
                "ip_address": "172.16.0.191"
            },
            {
                "subnet_id": "33ce2628-6246-4e3a-859f-99cd753ff704",
                "ip_address": "2001:db8:a583:21d:dfc0:d452:e9ab:65cf"
            }
        ],
        "mac_address": "fa:16:3e:1e:f7:9a",
        "network_id": "b0ad9b80-bb16-4550-8ce0-514f949e35ee",
        "tenant_id": "060576782980d5762f9ec014dd2f1148",
        "project_id": "060576782980d5762f9ec014dd2f1148",
        "device_id": "ab7ca781-66bf-48a8-814b-1568cb393a38",
        "device_owner": "compute:xxx",
        "security_groups": [
            "0552091e-b83a-49dd-88a7-4a5c86fd9ec3"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [{
         "ip_address": "1.1.1.1/0"
       }],
        "binding:vnic_type": "normal",
        "binding:vif_details": {
            "primary_interface": true
        },
        "binding:profile": {},
        "port_security_enabled": true,
        "dns_assignment": [
            {
                "hostname": "ip-172-16-0-191",
```



```
                "ip_address": "172.16.0.191",
                "fqdn": "ip-172-16-0-191.br-iaas-odin1.compute.internal."
            }
        ],
        "dns_name": "ip-172-16-0-191",
        "created_at": "2020-11-19T13:32:37",
        "updated_at": "2020-11-19T13:33:50"

    }
}
```


- For details about the error codes displayed if the request fails, see section **Error Codes**.

8 Permissions Policies and Supported Actions

8.1 Introduction

By default, new IAM users do not have permissions assigned. You need to add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups. This way, they can perform specified operations on cloud services based on the permissions.

You can grant users permissions using **roles** and **policies**. Roles are provided by IAM to define service-based permissions that match user's job responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

NOTE

If you want to allow or deny the access to an API, use policy-based authorization.

An account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user wants to query VPCs using an API, the user must have been granted permissions that allow the **vpc:vpcs:list** action.

Supported Actions

VPC provides system-defined policies that can be directly used in IAM. You can also create custom policies to supplement system-defined policies for more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: statements in a policy that allow or deny certain operations
- APIs: REST APIs that can be called by a user who has been granted specific permissions

- Actions: specific operations that are allowed or denied
- IAM project/Enterprise project: A custom policy can be applied to IAM projects or enterprise projects or both. Policies that contain actions supporting both IAM and enterprise projects can be assigned to user groups and take effect in both IAM and Enterprise Management. Policies that only contain actions supporting IAM projects can be assigned to user groups and only take effect for IAM. Such policies will not take effect if they are assigned to user groups in Enterprise Management. For details about the differences between IAM projects and enterprise projects, see **What Are the Differences Between IAM and Enterprise Management?**

  NOTE

  √: supported; x: not supported

8.2 VPC

Permission	API	Action
Creates a VPC.	POST /v1/{project_id}/vpcs	vpc:vpcs:create
Queries a VPC.	GET /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:get
Queries VPCs.	GET /v1/{project_id}/vpcs	vpc:vpcs:list
Updates a VPC.	PUT /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:update
Deletes a VPC.	DELETE /v1/{project_id}/vpcs/{vpc_id}	vpc:vpcs:delete

8.3 Subnet

Permission	API	Action
Creates a subnet.	POST /v1/{project_id}/subnets	vpc:subnets:create
Queries a subnet.	GET /v1/{project_id}/subnets/{subnet_id}	vpc:subnets:get
Queries subnets.	GET /v1/{project_id}/subnets	vpc:subnets:get
Updates a subnet.	PUT /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}	vpc:subnets:update
Deletes a subnet.	DELETE /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}	vpc:subnets:delete

8.4 Port

Permission	API	Action
Queries a port.	GET /v1/{project_id}/ports	vpc:ports:get
Queries port details.	GET /v1/{project_id}/ports/{port_id}	vpc:ports:get
Updates a port.	PUT /v1/{project_id}/ports/{port_id}	vpc:ports:update
Deletes a port.	DELETE /v1/{project_id}/ports/{port_id}	vpc:ports:delete
Creates a port.	POST / v1/{project_id}/ports	vpc:ports:create

8.5 VPC Peering Connection

Permission	API	Action
Querying VPC peering connections	GET /v2.0/vpc/peerings	vpc:peerings:get
Querying a VPC peering connection	GET /v2.0/vpc/peerings/{peering_id}	vpc:peerings:get
Creating a VPC peering connection	POST /v2.0/vpc/peerings	vpc:peerings:create
Accepting a VPC peering connection	PUT /v2.0/vpc/peerings/{peering_id}/accept	vpc:peerings:accept
Refusing a VPC peering connection	PUT /v2.0/vpc/peerings/{peering_id}/reject	vpc:peerings:reject
Updating a VPC peering connection	PUT /v2.0/vpc/peerings/{peering_id}	vpc:peerings:update
Deleting a VPC peering connection	DELETE /v2.0/vpc/peerings/{peering_id}	vpc:peerings:delete

8.6 VPC Route

Permission	API	Action
Querying VPC Routes	GET /v2.0/vpc/routes	vpc:routes:list
Querying a VPC Route	GET /v2.0/vpc/routes/{route_id}	vpc:routes:get
Creating a VPC Route	POST /v2.0/vpc/routes	vpc:routes:create
Deleting a VPC Route	DELETE /v2.0/vpc/routes/{route_id}	vpc:routes:delete

8.7 Route Table

Permission	API	Action
Querying Route Tables	GET /v1/{project_id}/routetables	vpc:routeTables:list
Querying a Route Table	GET /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:get
Creating a Route Table	POST /v1/{project_id}/routetables	vpc:routeTables:create
Updating a Route Table	PUT /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:update
Associating Subnets with a Route Table	POST /v1/{project_id}/routetables/{routetable_id}/action	vpc:routeTables:associate
Disassociating Subnets from a Route Table	POST /v1/{project_id}/routetables/{routetable_id}/action	vpc:routeTables:associate
Deleting a Route Table	DELETE /v1/{project_id}/routetables/{routetable_id}	vpc:routeTables:delete

8.8 Quota

Permission	API	Action
Queries quotas.	GET /v1/{project_id}/quotas	vpc:quotas:list

8.9 Private IP Address

Permission	API	Action
Assigns a private IP address.	POST /v1/{project_id}/privateips	vpc:privateIps:create
Queries a private IP address.	GET /v1/{project_id}/privateips/{privateip_id}	vpc:privateIps:get
Queries private IP addresses.	GET /v1/{project_id}/subnets/{subnet_id}/privateips	vpc:privateIps:list
Deletes a private IP address.	DELETE /v1/{project_id}/privateips/{privateip_id}	vpc:privateIps:delete

8.10 Security Group

Permission	API	Action
Creates a security group.	POST /v1/{project_id}/security-groups	vpc:securityGroups:create
Queries a security group.	GET /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:get
Queries security groups.	GET /v1/{project_id}/security-groups	vpc:securityGroups:get
Deletes a security group.	DELETE /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:delete

8.11 Security Group Rule

Permission	API	Action
Creates a security group rule.	POST /v1/{project_id}/security-group-rules	vpc:securityGroupRules:create
Queries a security group rule.	GET /v1/{project_id}/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:get
Queries security group rules.	GET /v1/{project_id}/security-group-rules	vpc:securityGroupRules:get
Deletes a security group rule.	DELETE /v1/{project_id}/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:delete
Updates a security group rule.	-	vpc:securityGroupRules:update

8.12 VPC Tags

Permission	API	Action
Creating a Tag for a VPC	POST /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcTags:create
Querying VPC Tags	GET /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcTags:get
Deleting a VPC Tag	DELETE /v2.0/{project_id}/vpcs/{vpc_id}/tags/{key}	vpc:vpcTags:delete
Batch Creating or Deleting VPC Tags	POST /v2.0/{project_id}/vpcs/{vpc_id}/tags/action	vpc:vpcTags:create vpc:vpcTags:delete
Querying VPCs by Tag	POST /v2.0/{project_id}/vpcs/resource_instances/action	vpc:vpcTags:get
Querying VPC Tags in a Specified Project	GET /v2.0/{project_id}/vpcs/tags	vpc:vpcTags:get

8.13 Subnet Tags

Permission	API	Action
Creating a Tag for a Subnet	POST /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnetTags:create
Querying Subnet Tags	GET /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnetTags:get
Deleting a Subnet Tag	DELETE /v2.0/{project_id}/subnets/{subnet_id}/tags/{key}	vpc:subnetTags:delete
Batch Creating or Deleting Subnet Tags	POST /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnetTags:create vpc:subnetTags:delete
Querying Subnets by Tag	POST /v2.0/{project_id}/subnets/resource_instances/action	vpc:subnetTags:get
Querying Subnet Tags in a Specified Project	GET /v2.0/{project_id}/subnets/tags	vpc:subnetTags:get

8.14 VPC Flow Log

Permission	API	Action
Creating a VPC Flow Log	POST /v1/{project_id}/fl/flow_logs	vpc:flowLogs:create
Querying VPC Flow Logs	GET /v1/{project_id}/fl/flow_logs	vpc:flowLogs:get
Querying a VPC Flow Log	GET /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:get
Updating a VPC Flow Log	PUT /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:update
Deleting a Flow Log	DELETE /v1/{project_id}/fl/flow_logs/{flowlog_id}	vpc:flowLogs:delete

8.15 Port (OpenStack Neutron API)

Permission	API	Action
Queries ports.	GET /v2.0/ports	vpc:ports:get
Queries a port.	GET /v2.0/ports/{port_id}	vpc:ports:get
Creates a port.	POST /v2.0/ports	vpc:ports:create
Updates a port.	PUT /v2.0/ports/{port_id}	vpc:ports:update
Deletes a port.	DELETE /v2.0/ports/{port_id}	vpc:ports:delete

8.16 Network (OpenStack Neutron API)

Permission	API	Action
Queries networks.	GET /v2.0/networks	vpc:networks:get
Queries a network.	GET /v2.0/networks/{network_id}	vpc:networks:get
Creates a network.	POST /v2.0/networks	vpc:networks:create
Updates a network.	PUT /v2.0/networks/{network_id}	vpc:networks:update
Deletes a network.	DELETE /v2.0/networks/{network_id}	vpc:networks:delete

8.17 Subnet (OpenStack Neutron API)

Permission	API	Action
Queries subnets.	GET /v2.0/subnets	vpc:subnets:get
Queries a subnet.	GET /v2.0/subnets/{subnet_id}	vpc:subnets:get

Permission	API	Action
Creates a subnet.	POST /v2.0/subnets	vpc:subnets:create
Updates a subnet.	PUT /v2.0/subnets/{subnet_id}	vpc:subnets:update
Deletes a subnet.	DELETE /v2.0/subnets/{subnet_id}	vpc:subnets:delete

8.18 Router (OpenStack Neutron API)

Permission	API	Action
Queries routers.	GET /v2.0/routers	vpc:routers:get
Queries a router.	GET /v2.0/routers/{router_id}	vpc:routers:get
Creates a router.	POST /v2.0/routers	vpc:routers:create
Updates a router.	PUT /v2.0/routers/{router_id}	vpc:routers:update
Deletes a router.	DELETE /v2.0/routers/{router_id}	vpc:routers:delete
Adds an interface to a router.	PUT /v2.0/routers/{router_id}/add_router_interface	• vpc:routers:addInterface • vpc:routers:get
Removes an interface from a router.	PUT /v2.0/routers/{router_id}/remove_router_interface	• vpc:routers:removeInterface • vpc:routers:get

8.19 Network ACL (OpenStack Neutron API)

Permission	API	Action
Queries all network ACL rules.	GET /v2.0/fwaas/firewall_rules	vpc:firewallRules:get
Queries a network ACL rule.	GET /v2.0/fwaas/firewall_rules/{firewall_rule_id}	vpc:firewallRules:get

Permission	API	Action
Creates a network ACL rule.	POST /v2.0/fwaas/firewall_rules	vpc:firewallRules:create
Updates a network ACL rule.	PUT /v2.0/fwaas/firewall_rules/{firewall_rule_id}	vpc:firewallRules:update
Deletes a network ACL rule.	DELETE /v2.0/fwaas/firewall_rules/{firewall_rule_id}	vpc:firewallRules:delete
Queries all network ACL policies.	GET /v2.0/fwaas/firewall_policies	vpc:firewallPolicies:get
Queries a network ACL policy.	GET /v2.0/fwaas/firewall_policies/{firewall_policy_id}	vpc:firewallPolicies:get
Creates a network ACL policy.	POST /v2.0/fwaas/firewall_policies	vpc:firewallPolicies:create
Updates a network ACL policy.	PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}	vpc:firewallPolicies:update
Deletes a network ACL policy.	DELETE /v2.0/fwaas/firewall_policies/{firewall_policy_id}	vpc:firewallPolicies:delete
Inserts a network ACL rule.	PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}/insert_rule	• vpc:firewallPolicies:addRule • vpc:firewallPolicies:get
Removes a network ACL rule.	PUT /v2.0/fwaas/firewall_policies/{firewall_policy_id}/remove_rule	• vpc:firewallPolicies:removeRule • vpc:firewallPolicies:get
Queries all network ACL groups.	GET /v2.0/fwaas/firewall_groups	vpc:firewallGroups:get
Queries a network ACL group.	GET /v2.0/fwaas/firewall_groups/{firewall_group_id}	vpc:firewallGroups:get
Creates a network ACL group.	POST /v2.0/fwaas/firewall_groups	vpc:firewallGroups:create

Permission	API	Action
Updates a network ACL group.	PUT /v2.0/fwaas/firewall_groups/{firewall_group_id}	vpc:firewallGroups:update
Deletes a network ACL group	DELETE /v2.0/fwaas/firewall_groups/{firewall_group_id}	vpc:firewallGroups:delete

8.20 Security Group (OpenStack Neutron API)

Permission	API	Action
Queries a security group.	GET /v2.0/security-groups	vpc:securityGroups:get
Queries details about a security group.	GET /v2.0/security-groups/{security_group_id}	vpc:securityGroups:get
Creates a security group.	POST /v2.0/security-groups	vpc:securityGroups:create
Updates a security group.	PUT /v2.0/security-groups/{security_group_id}	vpc:securityGroups:update
Deletes a security group.	DELETE /v2.0/security-groups/{security_group_id}	vpc:securityGroups:delete
Queries a security group rule.	GET /v2.0/security-group-rules	vpc:securityGroupRules:get
Queries details about a security group rule.	GET /v2.0/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:get
Creates a security group rule.	POST /v2.0/security-group-rules	vpc:securityGroupRules:create
Deletes a security group rule.	DELETE /v2.0/security-group-rules/{rules_security_groups_id}	vpc:securityGroupRules:delete

8.21 Precautions for API Permissions

If you have insufficient permissions, response code **200** will be returned when you query network resources and an empty list will be displayed.

9 FAQs

9.1 What Is the Difference Between the VPC Subnet API and the OpenStack Neutron Subnet API?

Difference

Subnet APIs are classified into **VPC subnet APIs** and **OpenStack Neutron subnet APIs**. They can create, query, update, and delete subnets.

The differences between the two are the meanings of the network ID and subnet ID.

Log in to the management console and view the basic information about the subnet. **Network ID** and **Subnet ID** are displayed.

Figure 9-1 Basic subnet information

- The subnet ID used when calling the VPC subnet API is the network ID shown in **Figure 9-1**. For example, a22724a0-b77b-44b4-b731-afd3a4839863.
- The subnet ID used when calling the OpenStack Neutron subnet API is the subnet ID shown in **Figure 9-1**. For example, f32a3acf-2312-41d0-947c-13d377a35059.

Example

The following queries subnet details to compare the difference.

VPC subnet API


```
GET /v1/049d06b7f20037e12f0dc0137381822f/subnets/a22724a0-b77b-44b4-b731-afd3a4839863
{
    "subnet": {
        "id": "a22724a0-b77b-44b4-b731-afd3a4839863",  //Correspond to the network ID on the
management console.
        "name": "subnet-54eb",
        "description": "",
        "cidr": "192.168.0.0/24",
        "dnsList": [
            "100.125.1.202",
            "100.125.1.230"
        ],
        "status": "ACTIVE",
        "tags": [],
        "vpc_id": "f4d0ebd4-2a62-4396-980b-96e73b3386de",
        "ipv6_enable": false,
        "gateway_ip": "192.168.0.1",
        "dhcp_enable": true,
        "primary_dns": "100.125.1.202",
        "secondary_dns": "100.125.1.230",
        "availability_zone": "az1.dc1",
        "neutron_network_id": "a22724a0-b77b-44b4-b731-afd3a4839863",  //Correspond to the network ID
on the management console.
        "neutron_subnet_id": "f32a3acf-2312-41d0-947c-13d377a35059",  //Correspond to the subnet ID on
the management console.
        "extra_dhcp_opts": []
    }
}
```

OpenStack Neutron subnet API

```
GET /v2.0/subnets/f32a3acf-2312-41d0-947c-13d377a35059
{
    "subnet": {
        "name": "subnet-54eb",
        "cidr": "192.168.0.0/24",
        "id": "f32a3acf-2312-41d0-947c-13d377a35059",  //Correspond to the subnet ID on the management
console.
        "enable_dhcp": true,
        "network_id": "a22724a0-b77b-44b4-b731-afd3a4839863",  //Correspond to the network ID on the
management console.
        "tenant_id": "049d06b7f20037e12f0dc0137381822f",
        "project_id": "049d06b7f20037e12f0dc0137381822f",
        "dns_nameservers": [
            "100.125.1.202",
            "100.125.1.230"
        ],
        "allocation_pools": [
            {
                "start": "192.168.0.2",
                "end": "192.168.0.252"
            }
        ],
        "host_routes": [],
        "ip_version": 4,
        "gateway_ip": "192.168.0.1",
        "created_at": "2019-04-09T08:03:58",
        "updated_at": "2019-04-09T08:03:59"
    }
}
```


9.2 What Are the Relationships Among Network ACL Groups, Policies, and Rules?

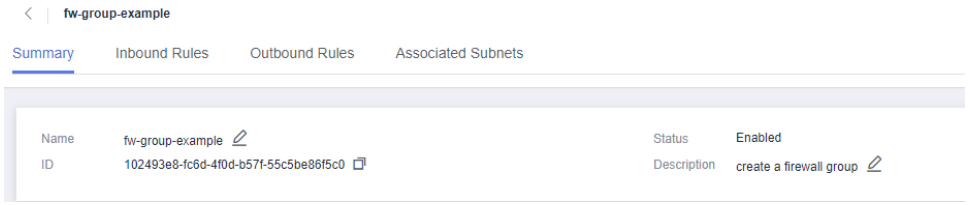
Relationships

Network ACL resources are classified into groups, policies, and rules.

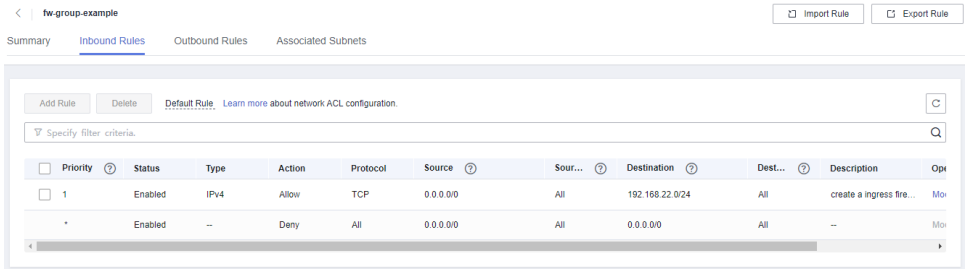
The relationships among them are as follows:

- A network ACL policy can be associated with multiple network ACL rules.
- A network ACL group can be associated with two network ACL policies. One policy controls inbound traffic and the other controls outbound traffic.
- A network ACL policy must be associated with a network ACL group.

Log in to the network console and view basic information about the network ACL. You can view the name and ID of the network ACL.



On the **Inbound Rules** or **Outbound Rules** tab, you can add, modify, or delete network ACL rules. These rules are associated with the same inbound or outbound policy.



Example

The following describes how to create network ACL resources.

- Creating a network ACL rule

```
POST /v2.0/fwaas/firewall_rules
```

Request body

```
{
    "firewall_rule": {
        "name": "fw-rule-ingress-1",
        "description": "create a ingress firewall rule ",
        "protocol": "TCP",
        "action": "ALLOW",
```



```
    "ip_version": 4,
    "destination_ip_address": "192.168.22.0/24",
    "source_ip_address": "0.0.0.0/0",
    "enabled": true
  }
}
```

Response body of obtaining **firewall_rule_id**: 84d10f4a-9f8b-41b8-bdfa-5a0f18736f12

```
{
  "firewall_rule": {
    "protocol": "tcp",
    "description": "create a ingress firewall rule ",
    "source_ip_address": "0.0.0.0/0",
    "destination_ip_address": "192.168.22.0/24",
    "source_port": null,
    "destination_port": null,
    "id": "84d10f4a-9f8b-41b8-bdfa-5a0f18736f12",
    "name": "fw-rule-ingress-1",
    "tenant_id": "5f6387106c2048b589b369d96c2f23a2",
    "project_id": "5f6387106c2048b589b369d96c2f23a2",
    "enabled": true,
    "action": "allow",
    "ip_version": 4,
    "public": false
  }
}
```

- Creating a network ACL policy

```
POST /v2.0/fwaas/firewall_policies
```

Request body of associating with a network ACL rule

```
{
  "firewall_policy": {
    "description": "create a ingress firewall policy",
    "firewall_rules": [
      "84d10f4a-9f8b-41b8-bdfa-5a0f18736f12"
    ],
    "name": "fw-policy-ingress"
  }
}
```

Response body of obtaining **firewall_policy_id**: da037721-b895-4e07-bbcc-f5f6ac2759fb

```
{
  "firewall_policy": {
    "id": "da037721-b895-4e07-bbcc-f5f6ac2759fb",
    "name": "fw-policy-ingress",
    "project_id": "5f6387106c2048b589b369d96c2f23a2",
    "tenant_id": "5f6387106c2048b589b369d96c2f23a2",
    "description": "create a ingress firewall policy",
    "firewall_rules": [
      "84d10f4a-9f8b-41b8-bdfa-5a0f18736f12"
    ],
    "audited": false,
    "public": false
  }
}
```

- Creating a network ACL group

```
POST /v2.0/fwaas/firewall_groups
```

Request body of associating with an inbound network ACL policy

```
{
  "firewall_group": {
```

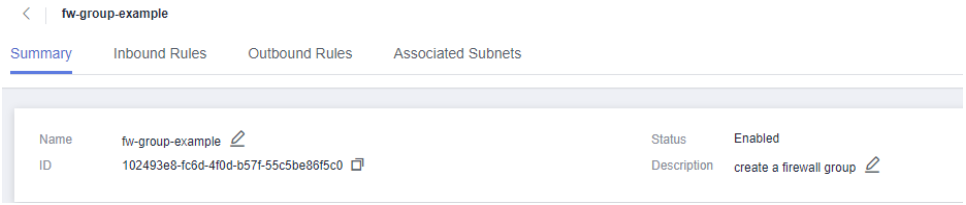


```
    "name": "fw-group-example",
    "description": "create a firewall group",
    "ingress_firewall_policy_id": "da037721-b895-4e07-bbcc-f5f6ac2759fb",
    "admin_state_up": true
  }
}
```

Response body of obtaining **firewall_group_id**: 102493e8-fc6d-4f0d-b57f-55c5be86f5c0.

```
{
  "firewall_group": {
    "id": "102493e8-fc6d-4f0d-b57f-55c5be86f5c0",
    "name": "fw-group-example",
    "project_id": "5f6387106c2048b589b369d96c2f23a2",
    "tenant_id": "5f6387106c2048b589b369d96c2f23a2",
    "admin_state_up": true,
    "egress_firewall_policy_id": null,
    "ingress_firewall_policy_id": "da037721-b895-4e07-bbcc-f5f6ac2759fb",
    "description": "create a firewall group",
    "created_at": "2023-03-09T08:54:40",
    "updated_at": "2023-03-09T08:54:40",
    "status": "INACTIVE",
    "ports": [],
    "public": false
  }
}
```

Log in to the network console and view the created network ACL resources.



10 Out-of-Date APIs

10.1 Port (Discarded)

10.1.1 Creating a Port (Discarded)

Function

This API is used to create a port.

URI

POST /v1/ports

Request Message

- Request parameter

Table 10-1 Request parameter

Name	Mandatory	Type	Description
port	Yes	**port** object	Specifies the port objects. For details, see **Table 10-2**.

Table 10-2 Description of the **port** field

Name	Mandatory	Type	Description
name	No	String	• Specifies the port name. • The value can contain no more than 255 characters. This parameter is left blank by default.
network_id	Yes	String	• Specifies the ID of the network to which the port belongs. • The network ID must be a real one in the network environment.
admin_state_up	No	Boolean	• Specifies the administrative state of the port. • The value can only be **true**, and the default value is **true**.
fixed_ips	No	Array of **fixed_ip** objects	• Specifies the port IP address. For details, see **Table 10-3**. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. • A port supports only one fixed IP address that cannot be changed.
tenant_id	No	String	Specifies the project ID.
security_groups	No	Array of strings	Specifies the UUID of the security group, for example, **"security_groups": ["a0608cbf-d047-4f54-8b28-cd7b59853fff"]**. This is an extended attribute.

Name	Mandatory	Type	Description
allowed_address_pairs	No	Array of **allow_address_pair** objects	• Specifies a set of zero or more allowed address pairs. An address pair consists of an IP address and MAC address. This attribute is extended. For details, see parameter **allow_address_pair** in **Table 10-4**. • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP.
port_security_enabled	No	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect. The default value is **true**.

Table 10-3 fixed_ip object

Name	Mandatory	Type	Description
subnet_id	No	String	• Specifies the subnet ID. • You cannot change the parameter value.

Name	Mandatory	Type	Description
ip_address	No	String	• Specifies the port IP address. • You cannot change the parameter value.

Table 10-4 allow_address_pair object

Name	Mandatory	Type	Description
ip_address	No	String	• Specifies the IP address. • You cannot set it to **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled.
mac_address	No	String	Specifies the MAC address.

Table 10-5 extra_dhcp_opt object

Name	Mandatory	Type	Description
opt_name	No	String	Specifies the option name.
opt_value	No	String	Specifies the option value.

- Example request

```
POST https://{Endpoint}/v1/ports

{
   "port": {
      "fixed_ips": [
         {
            "ip_address": "192.168.0.38",
            "subnet_id": "06bc2359-d75e-4f96-82f4-313e39c7148c"
         }
      ],
      "network_id": "28a1c93c-9a5e-4a9f-813b-e495bdef7d34",
      "security_groups": [
         "f2c5b3fc-b971-4a86-87b9-032586260e3e"
      ]
   }
}
```


Response Message

- Response parameter

Table 10-6 Response parameter

Name	Type	Description
port	**port** object	Specifies the port objects. For details, see **Table 10-7**.

Table 10-7 Description of the **port** field

Name	Type	Description
id	String	Specifies the port ID, which uniquely identifies the port.
name	String	• Specifies the port name. • The value can contain no more than 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network to which the port belongs. • The network ID must be a real one in the network environment.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The value can only be **true**, and the default value is **true**.
mac_address	String	• Specifies the port MAC address. • The system automatically sets this parameter, and you are not allowed to configure the parameter value.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. • A port supports only one fixed IP address that cannot be changed.

Name	Type	Description
device_id	String	• Specifies the ID of the device to which the port belongs. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
device_owner	String	• Specifies the belonged device, which can be the DHCP server, router, load balancer, or Nova. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
tenant_id	String	Specifies the project ID.
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always **DOWN**. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).
allowed_address_pairs	Array of **allow_address_pair** objects	• Specifies a set of zero or more allowed address pairs. An address pair consists of an IP address and MAC address. This attribute is extended. For details, see parameter **allow_address_pair** in **Table 10-9**. • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled.

Name	Type	Description
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 10-10**.
binding:vif_details	Object	Specifies the VIF details. Parameter **ovs_hybrid_plug** specifies whether the OVS/bridge hybrid mode is used.
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Instructions: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true }, Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.

Name	Type	Description
binding:vnic_type	String	• Specifies the type of the bound vNIC. • The value can be **normal** or **direct**. Parameter **normal** indicates software switching. Parameter **direct** indicates SR-IOV PCIe passthrough, which is not supported.
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect. The default value is **true**.

Table 10-8 fixed_ip object

Name	Type	Description
subnet_id	String	• Specifies the subnet ID. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 10-9 allow_address_pair object

Name	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24).
mac_address	String	Specifies the MAC address.

Table 10-10 extra_dhcp_opt object

Name	Type	Description
opt_name	String	Specifies the option name.

Name	Type	Description
opt_value	String	Specifies the option value.

- Example response

```
{
    "port": {
        "id": "d00f9c13-412f-4855-8af3-de5d8c24cd60",
        "name": "test",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
                "subnet_id": "70f2e74b-e660-410a-b754-0ca46744348a",
                "ip_address": "10.128.1.10"
            }
        ],
        "mac_address": "fa:16:3e:d7:f2:6c",
        "network_id": "5b808927-13c9-4e60-a4f4-ed6ffe225167",
        "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "02b4e8ee-74fa-4a31-802e-5490df11245e"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "binding:vif_details": {},
        "binding:profile": {},
        "port_security_enabled":true
    }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

10.1.2 Querying a Port (Discarded)

Function

This API is used to query a single port.

URI

GET /v1/ports/{port_id}

Table 10-11 describes the parameters.

Table 10-11 Parameter description

Name	Mandatory	Description
port_id	Yes	Specifies the port ID, which uniquely identifies the port.

Request Message

- Request parameter

  None

- Example request

```
GET https://{Endpoint}/v1/ports/d00f9c13-412f-4855-8af3-de5d8c24cd60
```

Response Message

- Response parameter

Table 10-12 Response parameter

Name	Type	Description
port	**port** object	Specifies the port objects. For details, see **Table 10-13**.

Table 10-13 Description of the **port** field

Name	Type	Description
id	String	Specifies the port ID, which uniquely identifies the port.
name	String	• Specifies the port name. • The value can contain no more than 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network to which the port belongs. • The network ID must be a real one in the network environment.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The value can only be **true**, and the default value is **true**.

Name	Type	Description
mac_address	String	• Specifies the port MAC address. • The system automatically sets this parameter, and you are not allowed to configure the parameter value.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. For details, see **Table 10-14**. • A port supports only one fixed IP address that cannot be changed.
device_id	String	• Specifies the ID of the device to which the port belongs. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
device_owner	String	• Specifies the belonged device, which can be the DHCP server, router, load balancer, or Nova. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
tenant_id	String	Specifies the project ID.
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always DOWN. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).

Name	Type	Description
allowed_address_pairs	Array of **allow_address_pair** objects	• Specifies a set of zero or more allowed address pairs. An address pair consists of an IP address and MAC address. This attribute is extended. For details, see parameter **allow_address_pair** in **Table 10-15**. • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 10-16**.
binding:vif_details	Object	Specifies the VIF details. Parameter **ovs_hybrid_plug** specifies whether the OVS/bridge hybrid mode is used.

Name	Type	Description
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Instructions: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true }, Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • The value can be **normal** or **direct**. Parameter **normal** indicates software switching. Parameter **direct** indicates SR-IOV PCIe passthrough, which is not supported.

Name	Type	Description
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect. The default value is **true**.

Table 10-14 fixed_ip object

Name	Type	Description
subnet_id	String	• Specifies the subnet ID. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 10-15 allow_address_pair object

Name	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24).
mac_address	String	Specifies the MAC address.

Table 10-16 extra_dhcp_opt object

Name	Type	Description
opt_name	String	Specifies the option name.
opt_value	String	Specifies the option value.

- Example response

```
{
    "port": {
        "id": "d00f9c13-412f-4855-8af3-de5d8c24cd60",
        "name": "test",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
```



```
            "subnet_id": "70f2e74b-e660-410a-b754-0ca46744348a",
            "ip_address": "10.128.1.10"
        }
    ],
    "mac_address": "fa:16:3e:d7:f2:6c",
    "network_id": "5b808927-13c9-4e60-a4f4-ed6ffe225167",
    "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
    "device_id": "",
    "device_owner": "",
    "security_groups": [
        "02b4e8ee-74fa-4a31-802e-5490df11245e"
    ],
    "extra_dhcp_opts": [],
    "allowed_address_pairs": [],
    "binding:vnic_type": "normal",
    "binding:vif_details": {},
    "binding:profile": {},
    "port_security_enabled":true
  }
}
```

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

10.1.3 Querying Ports (Discarded)

Function

This API is used to query ports and to display the ports in a list.

URI

GET /v1/ports

Example:

```
GET https://{Endpoint}/v1/ports?
id={port_id}&name={port_name}&admin_state_up={is_admin_status_up}&network_id={network_id}&mac_address={port_mac}&device_id={port_device_id}&device_owner={device_owner}&status={port_status}&fixed_ips=ip_address={ip_address}&fixed_ips=subnet_id={subnet_id}
```

Table 10-17 describes the parameters.

Table 10-17 Parameter description

Name	Mandatory	Type	Description
id	No	String	Specifies that the port ID is used as the filter.

Name	Mandatory	Type	Description
name	No	String	• Specifies that the port name is used as the filter. • The value can contain no more than 255 characters.
admin_state_up	No	Boolean	Specifies that the administrative state is used as the filter.
network_id	No	String	Specifies that the network ID is used as the filter.
mac_address	No	String	Specifies that the MAC address is used as the filter.
device_id	No	String	Specifies that the device ID is used as the filter.
device_owner	No	String	Specifies that the device owner is used as the filter.
status	No	String	• Specifies that the status is used as the filter. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.

Name	Mandatory	Type	Description
marker	No	String	Specifies a resource ID for pagination query, indicating that the query starts from the next record of the specified resource ID. This parameter can work together with the parameter **limit**. • If parameters **marker** and **limit** are not passed, resource records on the first page will be returned. • If the parameter **marker** is not passed and the value of parameter **limit** is set to **10**, the first 10 resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the value of parameter **limit** is set to **10**, the 11th to 20th resource records will be returned. • If the value of the parameter **marker** is set to the resource ID of the 10th record and the parameter **limit** is not passed, resource records starting from the 11th records (including 11th) will be returned.
limit	No	Integer	Specifies the number of records that will be returned on each page. The value is from 0 to intmax (2^31-1). The default value is 2000. **limit** can be used together with **marker**. For details, see the parameter description of **marker**.

Name	Mandatory	Type	Description
fixed_ips	No	String	You can use **fixed_ips=ip_address** or **fixed_ips=subnet_id** for filtering.

Request Message

- Request parameter
  None
- Example request
  GET https://{Endpoint}/v1/ports

Response Message

- Response parameter

Table 10-18 Response parameter

Name	Type	Description
ports	Array of **port** objects	Specifies the port objects. For details, see **Table 10-19**.

Table 10-19 Description of the **port** field

Name	Type	Description
id	String	Specifies the port ID, which uniquely identifies the port.
name	String	• Specifies the port name. • The value can contain no more than 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network to which the port belongs. • The network ID must be a real one in the network environment.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The value can only be **true**, and the default value is **true**.

Name	Type	Description
mac_address	String	• Specifies the port MAC address. • The system automatically sets this parameter, and you are not allowed to configure the parameter value.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. For details, see **Table 10-20**. • A port supports only one fixed IP address that cannot be changed.
device_id	String	• Specifies the ID of the device to which the port belongs. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
device_owner	String	• Specifies the belonged device, which can be the DHCP server, router, load balancer, or Nova. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
tenant_id	String	Specifies the project ID.
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always DOWN. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).

Name	Type	Description
allowed_address_pairs	Array of **allow_address_pair** objects	• Specifies a set of zero or more allowed address pairs. An address pair consists of an IP address and MAC address. This attribute is extended. For details, see parameter **allow_address_pair** in **Table 10-21**. • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 10-22**.
binding:vif_details	Object	Specifies the VIF details. Parameter **ovs_hybrid_plug** specifies whether the OVS/bridge hybrid mode is used.

Name	Type	Description
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Instructions: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true }, Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • The value can be **normal** or **direct**. Parameter **normal** indicates software switching. Parameter **direct** indicates SR-IOV PCIe passthrough, which is not supported.

Name	Type	Description
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect. The default value is **true**.

Table 10-20 fixed_ip object

Name	Type	Description
subnet_id	String	• Specifies the subnet ID. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 10-21 allow_address_pair object

Name	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24).
mac_address	String	Specifies the MAC address.

Table 10-22 extra_dhcp_opt object

Name	Type	Description
opt_name	String	Specifies the option name.
opt_value	String	Specifies the option value.

- Example response

```
{
   "ports": [
      {
         "id": "d00f9c13-412f-4855-8af3-de5d8c24cd60",
         "name": "test",
         "status": "DOWN",
         "admin_state_up": "true",
         "fixed_ips": [
```



```
            {
                "subnet_id": "70f2e74b-e660-410a-b754-0ca46744348a",
                "ip_address": "10.128.1.10"
            }
        ],
        "mac_address": "fa:16:3e:d7:f2:6c",
        "network_id": "5b808927-13c9-4e60-a4f4-ed6ffe225167",
        "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "02b4e8ee-74fa-4a31-802e-5490df11245e"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "binding:vif_details": {},
        "binding:profile": {},
        "port_security_enabled":true
    },
    {
        "id": "28ba8f45-7636-45e4-8c0a-675d7663717c",
        "name": "test1",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
                "subnet_id": "061d3ca2-bd1f-4bd1-a01d-7a5155328c0e",
                "ip_address": "192.168.10.10"
            }
        ],
        "mac_address": "fa:16:3e:3d:91:cd",
        "network_id": "be2fe79a-3ee2-4d87-bd71-5afa78a5670d",
        "tenant_id": "43f2d1cca56a40729dcb17212482f34d",
        "device_id": "",
        "device_owner": "",
        "security_groups": [
            "0bfc8687-ca18-4c37-ac84-d2198baba585"
        ],
        "extra_dhcp_opts": [],
        "allowed_address_pairs": [],
        "binding:vnic_type": "normal",
        "binding:vif_details": {},
        "binding:profile": {},
        "port_security_enabled":true
    }
  ]
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

10.1.4 Updating a Port (Discarded)

Function

This API is used to update a port.

URI

PUT /v1/ports/{port_id}

Table 10-23 describes the parameters.

Table 10-23 Parameter description

Name	Mandatory	Description
port_id	Yes	Specifies the port ID, which uniquely identifies the port.

Request Message

- Request parameter

Table 10-24 Request parameter

Name	Mandatory	Type	Description
port	Yes	**port** object	Specifies the port objects. For details, see **Table 10-25**.

Table 10-25 Description of the **port** field

Name	Mandatory	Type	Description
name	No	String	• Specifies the port name. • The value can contain no more than 255 characters. This parameter is left blank by default.
security_groups	No	Array of strings	Specifies the security group UUID.

Name	Mandatory	Type	Description
allowed_address_pairs	No	Array of **allow_address_pair** objects	• Specifies a set of zero or more allowed address pairs. An address pair consists of an IP address and MAC address. For details, see parameter **allow_address_pair** in **Table 10-26**. • Constraints: – The IP address cannot be **0.0.0.0**. – Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). – If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled. – To assign a virtual IP address to an ECS, the IP address configured in **allowed_address_pairs** must be an existing ECS NIC IP address. Otherwise, the virtual IP address cannot be used for communication.
extra_dhcp_opts	No	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 10-27**.

Table 10-26 allow_address_pair object

Name	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24).
mac_address	String	Specifies the MAC address.

Table 10-27 extra_dhcp_opt object

Name	Mandatory	Type	Description
opt_name	No	String	Specifies the option name.
opt_value	No	String	Specifies the option value.

- Example request

```
{
    "port": {
        "name": "adc"
    }
}
```

Response Message

- Response parameter

Table 10-28 Response parameter

Name	Type	Description
port	**port** object	Specifies the port objects. For details, see **Table 10-29**.

Table 10-29 Description of the **port** field

Name	Type	Description
id	String	Specifies the port ID, which uniquely identifies the port.

Name	Type	Description
name	String	• Specifies the port name. • The value can contain no more than 255 characters. This parameter is left blank by default.
network_id	String	• Specifies the ID of the network to which the port belongs. • The network ID must be a real one in the network environment.
admin_state_up	Boolean	• Specifies the administrative state of the port. • The value can only be **true**, and the default value is **true**.
mac_address	String	• Specifies the port MAC address. • The system automatically sets this parameter, and you are not allowed to configure the parameter value.
fixed_ips	Array of **fixed_ip** objects	• Specifies the port IP address. For example, the value is **"fixed_ips": [{"subnet_id": "4dc70db6-cb7f-4200-9790-a6a910776bba", "ip_address": "192.169.25.79"}]**. • A port supports only one fixed IP address that cannot be changed.
device_id	String	• Specifies the ID of the device to which the port belongs. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
device_owner	String	• Specifies the belonged device, which can be the DHCP server, router, load balancer, or Nova. • The system automatically sets this parameter, and you are not allowed to configure or change the parameter value.
tenant_id	String	Specifies the project ID.

Name	Type	Description
status	String	• Specifies the port status. The status of a HANA SR-IOV VM port is always **DOWN**. • The value can be **ACTIVE**, **BUILD**, or **DOWN**.
security_groups	Array of strings	Specifies the security group UUID (extended attribute).
allowed_address_pairs	Array of **allow_address_pair** objects	• Specifies a set of zero or more allowed address pairs. An address pair consists of an IP address and MAC address. This attribute is extended. For details, see parameter **allow_address_pair** in **Table 10-9**. • The IP address cannot be **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24). • If the value of **allowed_address_pairs** is **1.1.1.1/0**, the source/destination check is disabled.
extra_dhcp_opts	Array of **extra_dhcp_opt** objects	Specifies the extended option (extended attribute) of DHCP. For details, see **Table 10-10**.
binding:vif_details	Object	Specifies the VIF details. Parameter **ovs_hybrid_plug** specifies whether the OVS/bridge hybrid mode is used.

Name	Type	Description
binding:profile	Object	Specifies the user-defined settings. This is an extended attribute. Instructions: • The **internal_elb** field is in boolean type and is available to common tenants. Set the value of this parameter to **true** only when you assign a virtual IP address to an internal network load balancer. Common tenants do not have the permission to change the value of this field, which is maintained by the system. Example: {"internal_elb": true} • The **disable_security_groups** field is in boolean type and is available to common tenants. The default value is **false**. In high-performance communication scenarios, you can set the parameter value to **true**, which makes this parameter to be available to common tenants. You can specify this parameter when creating a port. Currently, the value of this parameter can only be set to **true**. Example: {"disable_security_groups": true }, Currently, the value can only be set to **true**. When the value is set to **true**, the FWaaS function does not take effect.
binding:vnic_type	String	• Specifies the type of the bound vNIC. • The value can be **normal** or **direct**. Parameter **normal** indicates software switching. Parameter **direct** indicates SR-IOV PCIe passthrough, which is not supported.

Name	Type	Description
port_security_enabled	Boolean	Specifies whether the security option is enabled for the port. If the option is not enabled, the security group and DHCP snooping do not take effect. The default value is **true**.

Table 10-30 fixed_ip object

Name	Type	Description
subnet_id	String	• Specifies the subnet ID. • You cannot change the parameter value.
ip_address	String	Specifies the port IP address.

Table 10-31 allow_address_pair object

Name	Type	Description
ip_address	String	• Specifies the IP address. • You cannot set it to **0.0.0.0**. • Configure a dedicated security group for the port if the parameter **allowed_address_pairs** has a large CIDR block (subnet mask less than 24).
mac_address	String	Specifies the MAC address.

Table 10-32 extra_dhcp_opt object

Name	Type	Description
opt_name	String	Specifies the option name.
opt_value	String	Specifies the option value.

- Example response

```
{
    "port": {
        "id": "7204e0da-40de-4207-a536-6f59b84f6f0e",
        "name": "adc",
        "status": "DOWN",
        "admin_state_up": "true",
        "fixed_ips": [
            {
```



```
            "subnet_id": "689156ca-038f-4478-b265-fd26aa8bbe31",
            "ip_address": "192.168.0.9"
        }
    ],
    "mac_address": "fa:16:3e:d7:f2:6c",
    "network_id": "b4152e98-e3af-4e49-bb7f-7766e2b5ec63",
    "tenant_id": "caa6cf4337ea47fb823b15709ebe8591",
    "device_id": "",
    "device_owner": "",
    "security_groups": [
        "59b39002-e79b-4bac-8e27-aa884ab1beb6"
    ],
    "extra_dhcp_opts": [],
    "allowed_address_pairs": [],
    "binding:vnic_type": "normal",
    "binding:vif_details": {},
    "binding:profile": {},
    "port_security_enabled":true
  }
}
```


Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

10.1.5 Deleting a Port (Discarded)

Function

This API is used to delete a port.

Restrictions

You are not allowed to delete the port if **device_owner** is specified.

URI

DELETE /v1/ports/{port_id}

Table 10-33 describes the parameters.

Table 10-33 Parameter description

Name	Mandatory	Description
port_id	Yes	Specifies the port ID, which uniquely identifies the port.

Request Message

- Request parameter

  None

- Example request
  None

Response Message

- Response parameter
  None
- Example response
  None

Status Code

See **Status Codes**.

Error Code

See **Error Codes**.

A Appendix

A.1 ICMP-Port Range Relationship Table

ICMP Type	port_range_min	port_range_max
Any	NULL	NULL
Echo	8	0
Echo reply	0	0
Fragment need DF set	3	4
Host redirect	5	1
Host TOS redirect	5	3
Host unreachable	3	1
Information reply	16	0
Information request	15	0
Net redirect	5	0
Net TOS redirect	5	2
Net unreachable	3	0
Parameter problem	12	0
Port unreachable	3	3
Protocol unreachable	3	2
Reassembly timeout	11	1
Source quench	4	0
Source route failed	3	5

ICMP Type	port_range_min	port_range_max
Timestamp reply	14	0
Timestamp request	13	0
TTL exceeded	11	0

A.2 VPC Monitoring Metrics

Description

This section describes monitoring metrics reported by VPC to Cloud Eye as well as their namespaces and dimensions. You can use APIs provided by Cloud Eye to query the monitoring metrics of the monitored object and alarms generated for VPC.

Namespace

SYS.VPCnetwork ACL

Metrics

Table A-1 EIP and bandwidth metrics

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic (Previously called "Upstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic (Previously called "Downstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth in the unit of percent. Outbound bandwidth usage = Outbound bandwidth/ Purchased bandwidth	0% to 100%	Bandwidth or EIP	1 minute
up_stream	Outbound Traffic	Network traffic going out of the cloud platform in a minute (Previously called "Upstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute
down_stream	Inbound Traffic	Network traffic going into the cloud platform in a minute (Previously called "Downstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute

Dimension

Key	Value
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

A.3 Status Codes

Table A-2 Normal values

Normal Response Code	Type	Description
200	OK	Specifies the normal response code for the GET, PUT, and POST operations.
201	Created	Specifies the normal response code for the POST operation of the OpenStack Neutron API and API V3.
204	No Content	Specifies the normal response code for the DELETE operation.

Table A-3 Abnormal values

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.
405 Method Not Allowed	You are not allowed to use the method specified in the request.
406 Not Acceptable	The response generated by the server could not be accepted by the client.
407 Proxy Authentication Required	You must use the proxy server for authentication so that the request can be processed.
408 Request Timeout	The request timed out.
409 Conflict	The request could not be processed due to a conflict.
500 Internal Server Error	Failed to complete the request because of an internal service error.

Returned Value	Description
501 Not Implemented	Failed to complete the request because the server does not support the requested function.
502 Bad Gateway	Failed to complete the request because the server has received an invalid response.
503 Service Unavailable	Failed to complete the request because the service is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

A.4 Error Codes

Description

If an error occurs when an API is called, error information is returned. This section describes the error information for VPC APIs (excluding native OpenStack APIs).

Example of Returned Error Information

```
{
    "code": "VPC.0002",
    "message": "Available zone Name is null."
}
```

Error Code Description

If an error code starting with **APIGW** is returned after you call an API, rectify the fault by referring to the instructions provided in **Error Codes**.

Module	Status Code	Error Code	Message	Description	Handling Measure
Public	400	VPC.0002	Available zone Name is null.	The AZ is left blank.	Check whether the **availability_zone** field in the request body for creating a subnet is left blank.

Module	Status Code	Error Code	Message	Description	Handling Measure
	404	VPC.0003	VPC does not exist.	The VPC does not exist.	Check whether the VPC ID is correct or whether the VPC exists under the tenant.
	400	VPC.0004	VPC is not active, please try later.	The VPC status is abnormal.	Try again later or contact technical support.
	401	VPC.0005	Lack of user authority.	User restricted.	Check whether the account is in arrears or has not applied for the OBT permission.
	401	VPC.0009	real-name authentication fail.	Real-name authentication fails.	Contact technical support.
Public	400	VPC.0007	urlTenantId is not equal tokenTenantId	Inconsistent tenant IDs.	The tenant ID in the URL is different from that parsed in the token.
	401	VPC.0008	Invalid token in the header.	Invalid token.	Check whether the token in the request header is valid.
	403	VPC.2701	Token not allowed to do this action.	You do not have permission to perform this operation, or your account balance is insufficient.	Check whether the account balance is insufficient or whether your account has been frozen.

Module	Status Code	Error Code	Message	Description	Handling Measure
Public	403	VPC.0010	Rules on xx by ** disallowed by policy	Insufficient permissions to make calls to the underlying system.	Obtain the required permissions.
	403	VPC.2201	Policy doesn't allow <x:x:x> to be performed	Insufficient fine-grained permissions.	Obtain the required permissions.
Public	400	VPC.0014	This enterpriseProject status is disable.	The enterprise project is unavailable.	Use the ID of another available enterprise project.
	400	VPC.0011	EnterpriseProjec-tId is invalid	Invalid enterprise project ID.	Enter a valid enterprise project ID.
Creating a port	400	VPC.2500	Param is invalid.	Invalid port parameter.	Check whether the parameter values are valid based on the returned error message and API reference document.
	409	VPC.0701	IP is in use	The IP address of the port has been used.	Change the IP address.
	409	VPC.2511	Quota exceeded for resources: ['vip'].	The maximum number of virtual IP addresses has been reached.	Delete virtual IP addresses that are no longer required.

Module	Status Code	Error Code	Message	Description	Handling Measure
	500	VPC.2502	The system error.	Calling the backend service fails.	Try again later or contact technical support.
Querying a port	404	VPC.2502	Port xx not found	The port does not exist.	Check whether the port exists.
	500	VPC.2502	The system error.	An error is returned for the failure to call the backend service.	Check whether the Neutron service is normal or contact technical support.
Querying ports	404	VPC.2502	Port xx not found	The port does not exist.	Check whether the port exists.
	500	VPC.2502	The system error.	An error is returned for the failure to call the backend service.	Check whether the Neutron service is normal or contact technical support.
Deleting a port	400	VPC.2500	Port's device_id is not empty.	Invalid parameters.	Check whether the parameter values are valid based on the returned error message.
	404	VPC.2502	Port xx not found	Invalid parameters.	Check whether the port exists.
	500	VPC.2502	Neutron Error.	Calling the backend service fails.	Try again later or contact technical support.

Module	Status Code	Error Code	Message	Description	Handling Measure
Creating a VPC	400	VPC.0101	Param is invalid.	VPC parameters are incorrect.	Check whether the parameter values are valid based on the returned error message and API reference document.
	409	VPC.0114	Quota exceeded for resources: ['router'].	The number of VPCs has reached the maximum allowed limit specified by the quota.	Clear VPC resources that no longer will be used or apply for expanding the VPC resource quota.
	400	VPC.0115	The router name has exist.	The VPC name already exists.	Change the VPC name.
Querying a VPC	400	VPC.0101	getVpc error vpcId is invalid.	VPC parameters are incorrect.	Ensure that the specified VPC ID is correct.
	404/500	VPC.0105	Neutron Error.	Calling the backend service fails.	Check whether the Neutron service is normal or contact technical support.
	500	VPC.0106	get router is null.	An error is returned for the failure to call the backend service.	Check whether the Neutron service is normal or contact technical support.

Module	Status Code	Error Code	Message	Description	Handling Measure
Querying VPCs	400	VPC.0101	Query vpc list error.	Failed to query the VPCs.	Check whether the parameter values are valid based on the returned error message.
	500	VPC.0105	Neutron Error.	Calling the backend service fails.	Check whether the Neutron service is normal or contact technical support.
	500	VPC.0106	query routers or getList are null.	The response result of calls to the IaaS OpenStack system is null or empty.	Check whether the Neutron service is normal or contact technical support.
Deleting a VPC	400/404	VPC.0101	Delete router error xx is invalid.	Invalid parameters.	Check whether the parameter values are valid based on the returned error message.
	500	VPC.0102	Delete router fail.	The interface fails to obtain the routing resources.	Contact technical support.

Module	Status Code	Error Code	Message	Description	Handling Measure
	409	VPC.0103	Resource status is busy. Try again later.	The VPC cannot be deleted because it is being created.	Contact technical support.
	409	VPC.0104	Router contains subnets, please delete subnet first.	The VPC cannot be deleted because it contains subnets.	Delete the subnet in the VPC.
	404/500	VPC.0105	Neutron Error.	Calling the backend service fails.	Check whether the Neutron service is normal or contact technical support.
	409	VPC.0107	Delete the firewall first before deleting the router.	Failed to delete the VPC because it has network ACLs associated.	Delete the network ACLs of the tenant first.
	409	VPC.0108	Router is used not allow deleted.	Failed to delete the VPC because it has EIPs associated.	Delete the EIPs of the tenant first.
	409	VPC.0110	deleteDefaultNetworkFromRouter router status is invalid.	The VPC cannot be deleted because its status is unstable.	Contact technical support.
	500	VPC.0111	Database Error.	An internal VPC exception occurs.	Contact technical support.

Module	Status Code	Error Code	Message	Description	Handling Measure
	409	VPC.0112	Delete the securitygroup first before deleting the router.	The VPC cannot be deleted because it contains security groups.	Delete security groups of the tenant.
	409	VPC.0118	ELB exists under this router, delete ELB firstly.	The VPC cannot be deleted because it contains load balancers.	Delete load balancers in the VPC.
	500	VPC.0119	ELB Error.	An error occurred when the VPC service makes calls to the ELB service.	Check whether the ELB service is normal or contact technical support.
	409	VPC.0120	exroutes exists under this router, delete exroutes firstly.	The VPC cannot be deleted because it contains extension routes.	Delete extension routes in the VPC.
Deleting a VPC	409	VPC.0109	Router is used not allow deleted.	Failed to delete the VPC because one or more VPNs have been created for it.	Delete VPNs of the tenant.
Updating a VPC	400	VPC.0101	Update router xx is invalid.	Invalid parameters.	Check whether the parameter values are valid based on the returned error message.

Module	Status Code	Error Code	Message	Description	Handling Measure
	404/500	VPC.0105	Neutron Error.	Calling the backend service fails.	Check whether the Neutron service is normal or contact technical support.
	500	VPC.0113	Router status is not active.	The VPC cannot be updated because the status of the VPC is abnormal.	Try again later or contact technical support.
	400	VPC.0115	The router name has exist.	The VPC name already exists.	Change the VPC name.
	400	VPC.0117	Cidr can not contain subnetList cidr.	The subnet parameters are invalid. The VPC CIDR block does not contain all its subnet CIDR blocks.	Change the CIDR block of the VPC.
Creating a subnet	400	VPC.0201	Subnet name is invalid.	Incorrect subnet parameters.	Check whether the parameter values are valid based on the returned error message and API reference document.
	500	VPC.0202	Create subnet failed.	An internal error occurs in the subnet.	Contact technical support.

Module	Status Code	Error Code	Message	Description	Handling Measure
	400	VPC.0203	Subnet is not in the range of VPC.	The CIDR block of the subnet is not in the range of the VPC.	Change the CIDR block of the subnet.
	400	VPC.0204	The subnet has already existed in the VPC, or has been in conflict with the VPC subnet.	The CIDR block of the subnet already exists in the VPC.	Change the CIDR block of the subnet.
	400	VPC.0212	The subnet cidr is not valid.	Invalid subnet CIDR block.	Check whether the subnet CIDR block is valid.
Querying a subnet	400	VPC.0201	Subnet ID is invalid.	Invalid subnet ID.	Check whether the subnet ID is valid.
	404/500	VPC.0202	Query subnet fail.	Failed to query the subnet.	Contact technical support.
Querying subnets	400	VPC.0201	Query subnets list error.	Failed to query the subnets.	Check whether the parameter values are valid based on the returned error message.
	500	VPC.0202	List subnets error.	Failed to query the subnets.	Contact technical support.
Deleting a subnet	400	VPC.0201	Subnet ID is invalid.	Invalid subnet ID.	Check whether the parameter values are valid based on the returned error message.

Module	Status Code	Error Code	Message	Description	Handling Measure
	404/500	VPC.0202	Neutron Error.	An internal error occurs in the subnet.	Contact technical support.
	400	VPC.0207	Subnet does not belong to the VPC.	This operation is not allowed because the subnet does not belong to the VPC.	Check whether the subnet is in the VPC.
	500	VPC.0208	Subnet is used by private IP, can not be deleted.	The subnet cannot be deleted because it is being used by the private IP address.	Delete the private IP address of the subnet.
	500	VPC.0209	subnet is still used ,such as computer,LB.	The subnet cannot be deleted because it is being used by an ECS or load balancer.	Delete the ECS or load balancer in the subnet.
	500	VPC.0210	Subnet has been used by routes, please remove the routes first and try again.	The subnet cannot be deleted because it is being used by the custom route.	Delete the custom route.
	500	VPC.0211	subnet is still used by LBaas.	The subnet cannot be deleted because it is being used by load balancers.	Delete load balancers in the subnet.

Module	Status Code	Error Code	Message	Description	Handling Measure
Deleting a subnet	500	VPC.0206	Subnet has been used by VPN, please remove the subnet from the VPN and try again.	The subnet cannot be deleted because it is being used by the VPN.	Delete the subnet that is used by the VPN.
Updating a subnet	400	VPC.0201	xx is invalid.	Incorrect subnet parameters.	Check whether the parameter values are valid based on the returned error message.
	404/500	VPC.0202	Neutron Error.	An internal error occurs in the subnet.	Contact technical support.
	500	VPC.0205	Subnet states is invalid, please try again later.	The subnet cannot be updated because it is being processed.	Try again later or contact technical support.
	400	VPC.0207	Subnet does not belong to the VPC.	This operation is not allowed because the subnet does not belong to the VPC.	Check whether the subnet is in the VPC.
Querying quotas	400	VPC.1207	resource type is invalid.	The specified resource type does not exist.	Use an existing resource type.
Assigning a private IP address	500	VPC.0701	The IP has been used.	The private IP address already exists.	Change another private IP address and try again.

Module	Status Code	Error Code	Message	Description	Handling Measure
	400	VPC.0705	IP address is not a valid IP for the specified subnet.	Invalid private IP address	Check whether the specified IP address in the request body is within the subnet CIDR block.
	404	VPC.2204	Query resource by id fail.	The resource does not exist or the permission is insufficient.	Check whether the specified subnet in the request body exists or the current account has the permission to query the subnet.
	409	VPC.0703	No more IP addresses available on network xxx.	Insufficient IP addresses.	Check whether the subnet has sufficient IP addresses.
Querying a Private IP Address	404	VPC.0704	Query resource by id fail.	The private IP address does not exist.	Check whether the private IP address exists.
Querying Private IP Addresses	400	VPC.0702	query privateIps error.	Invalid parameters.	Check whether the parameter values are valid based on the returned error message.
Releasing a Private IP Address	404	VPC.0704	Query resource by id fail.	The private IP address does not exist.	Check whether the private IP address exists.

Module	Status Code	Error Code	Message	Description	Handling Measure
	500	VPC.0706	Delete port fail.	An error occurs when the private IP address is being released.	Try again later or contact technical support.
	409	VPC.0707	privateIp is in use.	The private IP address is in use.	Check whether the private IP address is being used by other resource.
Creating a security group	400	VPC.0601	Creating securitygroup name is invalid.	The parameters of the security group are incorrect.	Check whether the parameter values are valid based on the returned error message and API reference document.
	500	VPC.0602	Add security group fail.	An internal error occurs in the security group.	Check whether the Neutron service is normal or contact technical support.
	409	VPC.0604	Quota exceeded for resources: ['security_group'].	Insufficient security group quota.	Delete the security group that is no longer required or apply for increasing the quota.

Module	Status Code	Error Code	Message	Description	Handling Measure
Querying a security group	400	VPC.0601	Securitygroup id is invalid.	The parameters of the security group are incorrect.	Check whether the security group ID is valid.
	500	VPC.0602	Query security group fail.	An internal error occurs in the security group.	Check whether the Neutron service is normal or contact technical support.
	404	VPC.0603	Securitygroup is not exist.	The security group does not exist.	Check whether the security group ID is correct or whether the security group exists under the tenant.
	404/500	VPC.0612	Neutron Error.	An internal error occurs in the security group.	Contact technical support.
Querying security groups	400	VPC.0601	Query security groups error limit is invalid.	The parameters of the security group are incorrect.	Check whether the parameter values are valid based on the returned error message and API reference document.

Module	Status Code	Error Code	Message	Description	Handling Measure
	500	VPC.0602	Query security groups fail.	An internal error occurs in the security group.	Check whether the Neutron service is normal or contact technical support.
Creating a security group rule	409	VPC.0602	1.Security group rule already exists. 2.Quota exceeded for resources: ['security_group_rule']. 3.Failed to create the security group rule concurrently. The rule already exists.	The security group rule already exists. Insufficient security group rule quota. Failed to create the security group rule concurrently. The rule already exists.	Change the request body for creating a security group rule. Delete the security group rule that is no longer required or apply for increasing the quota. Check whether the security group rules created concurrently are different from each other.
Route table	400	VPC.2800	Routetable ID is invalid.	Invalid route table parameters.	Ensure that the request parameters are correct.
	400/500	VPC.2801	NeutronError	Internal route table error.	Check the request parameters or contact technical support.
	404	VPC.2802	RouteTable is not exist	The route table could not be found.	Check whether the route table exists.

Module	Status Code	Error Code	Message	Description	Handling Measure
	400	VPC.2803	NeutronError	The destination of the route overlaps the subnet.	The destination of the route in the request parameters already exists.
	409	VPC.2804	The routetable that been bonded by subnet can't be deleted	Failed to delete the route table because it is associated with one or more subnets.	Disassociate the subnets from the route table and try again.
	500	VPC.2805	NeutronError	Failed to change the next hop of the route.	Contact technical support.
	500	VPC.2806	Query subnet id by network id failed for illegal argument	Failed to associate subnets with or disassociate them from the route table.	Contact technical support.
	400	VPC.2807	subnet not exist or not belong to the vpc, associate routertable failed	The subnet to be associated with the route table does not exist or does not belong to the VPC.	Check the request parameters or change the subnet to one in the VPC of the route table.
	404	VPC.2808	RouteTable is not exist	The route table could not be found.	Check whether the route table exists.

Module	Status Code	Error Code	Message	Description	Handling Measure
	400	VPC.2809	NeutronError	The destination of the route overlaps with that of a system route.	Ensure that the destination in each route is unique.
	400	VPC.2810	the vpc cannot support customized routetable	The current VPC does not support the custom route function.	Change the VPC or contact technical support.
	400	VPC.2811	InvalidVgwForRouteGateway	The virtual gateway of the current Direct Connect connection has not been associated with any device and the route cannot be delivered.	Select another Direct Connect connection.
	400	VPC.2812	The destination of route to add is exist already	The route destination already exists.	Use an available destination.
	400	VPC.2813	RoutePerRouteTableOverLimit	The route quota is insufficient.	Increase the route quota or select another route table.
	500	VPC.2814	internal server error	An internal processing error occurs in the route table.	Contact technical support.
	400	VPC.2815	DuplicatedDestination	The route destination already exists.	Use an available destination.

Module	Status Code	Error Code	Message	Description	Handling Measure
	400	VPC.2816	subnet has been bonded by routetable	The subnet has already been associated to a route table.	Disassociate the subnet, and then associate it with another route table.
Resource tags	400	VPC.1801	resource id is invalid.	Incorrect resource ID.	Use a correct resource ID.
	400	VPC.1801	action is invalid.	Invalid action value.	Ensure that the value of **action** is **create** or **delete**.
	400	VPC.1801	Tag length is invalid. The key length must be in range [1,36] and value in range [0,43]	Invalid key length. The key can contain 1 to 36 characters.	Use a valid key value.
	400	VPC.1801	Tag length is invalid. The key length must be in range [1,36] and value in range [0,43]	Invalid value length. The value can contain 0 to 43 characters.	Use a value of valid length.
	400	VPC.1801	Resource_type xxx is invalid.	Incorrect resource type.	Ensure that the value of **resource_type** is **vpcs**.
	400	VPC.1801	Tag can not be null.	The tag list contains value null.	Use valid tags.
	400	VPC.1801	The list of matches contains null.	The matches list contains value null.	Use valid matches.
	400	VPC.1801	Tag value can not be null.	The tags exist, but their values are null.	Use valid tags.

Module	Status Code	Error Code	Message	Description	Handling Measure
	400	VPC.1801	The value of Matches in resourceInstancesReq is null.	The matches exist, and the value is null.	Use valid matches.
	400	VPC.1801	number of tags exceeds max num of 10.	The tag list contains more than 10 keys.	Use valid tags.
	400	VPC.1801	Tag key is repeated.	The tag list contains duplicate keys.	Use valid tags.
	400	VPC.1801	Value of tags in resourceInstancesReq is duplicate.	There are duplicate tag values in the tag list.	Use valid tags.
	400	VPC.1801	number of tags exceeds max num of 10.	The tag in the tag list has more than 10 tag values.	Use valid tags.
	400	VPC.1801	The key of matches is invalid.	The key in **matches** is not the resource name.	Use valid matches.
	400	VPC.1801	Limit in resourceInstancesReq is invalid. Offset in resourceInstancesReq is invalid.	Invalid **limit** or **offset** value.	Use valid **limit** and **offset** values.
	400	VPC.1801	ResourceInstancesReq is null or invalid.	The tags dictionary structure is missing.	Use a valid tags dictionary structure.
	400	VPC.1801	Tag length is invalid. The key length must be in range [1,36] and value in range [0,43]	The key in tags exceeds the maximum length or is left blank.	Use valid keys in tags.

Module	Status Code	Error Code	Message	Description	Handling Measure
	400	VPC.1801	Tag length is invalid. The key length must be in range [1,36] and value in range [0,43]	A value in tags exceeds the maximum length.	Use valid values in tags.
	400	VPC.1801	ResourceInstancesReq is null or invalid.	The matches dictionary structure is missing.	Use a valid matches dictionary structure.
	400	VPC.1801	The number of Matches in resourceInstancesReq is 0.	The matches are an empty list.	Use a valid matches list.
	400	VPC.1801	The value's length of Matches in resourceInstancesReq is more than 255.	The matches list contains tag values that contain more than 255 Unicode characters.	Use a valid matches list.
	500	VPC.1801	InvalidInput	Incorrect request body format.	Use the correct request body format.
	404	VPC.2204	Query subnet by id fail.	The resource does not exist or the permission is insufficient.	Use an existing resource or obtain required permission.
Querying the network IP address usage	400	VPC.2301	parameter network_id is invalid.	The request parameter is incorrect.	Enter a valid network ID.
	400	VPC.2302	Network xxx could not be found.	The network is not found.	Ensure that the network ID exists.

Module	Status Code	Error Code	Message	Description	Handling Measure
Creating a VPC flow log	400	VPC.3001	resource_type/ log_store_type/ traffic_type/ log_group_id/ log_topic_id is invalid	Incorrect type or ID.	Check whether the type is supported or whether the ID format is correct.
	400	VPC.3002	Port does not support flow log, port id : xxx	The VPC flow log does not support this type of port.	Check whether the port is an S3, C3, or M3 ECS NIC port.
	404	VPC.3002	Port/Network/Vpc xxx could not be found.	The resource does not exist.	Check whether the resource exists.
	409	VPC.3004	Content of flow log is duplicate: resource type xxx, reousce id xxx, traffic type all, log group id xxx, log topic id xxx, log store type xxx, log store name xxx.	This VPC flow log already exists.	Modify the parameters of the VPC flow log.
	500	VPC.3002	Create flow log by xxx(tenant_id) fail.	Calling the backend service fails.	Try again later or contact technical support.
Querying VPC flow logs	404	VPC.3001	resource could not be found, xxx(listParam) is invalid	Invalid parameters.	Check whether the parameter format is correct.
	500	VPC.3002	Neutron Error.	Calling the backend service fails.	Try again later or contact technical support.

Module	Status Code	Error Code	Message	Description	Handling Measure
Querying a VPC flow log	404	VPC.3001	resource could not be found, flowlog id is invalid.	Invalid VPC flow log ID.	Check whether the VPC flow log ID format is correct.
	404	VPC.3002	Flow log xxx could not be found.	The VPC flow log does not exist.	Check whether the VPC flow log exists or whether its ID is correct.
Updating a VPC flow log	404	VPC.3001	resource could not be found, flowlog id is invalid.	Invalid VPC flow log ID.	Check whether the VPC flow log ID format is correct.
	404	VPC.3005	Flow log xxx could not be found.	The VPC flow log does not exist.	Check whether the VPC flow log exists or whether its ID is correct.
	500	VPC.3002	Update flow log by xxx(tenant_id) fail.	Calling the backend service fails.	Try again later or contact technical support.
Deleting a VPC flow log	404	VPC.3001	resource could not be found, flowlog id is invalid.	Invalid VPC flow log ID.	Check whether the VPC flow log ID format is correct.
	404	VPC.3005	Flow log xxx could not be found.	The VPC flow log does not exist.	Check whether the VPC flow log exists or whether its ID is correct.
	500	VPC.3002	Delete flow log by xxx(tenant_id) fail.	Calling the backend service fails.	Try again later or contact technical support.

A.5 Obtaining a Project ID

Scenarios

A project ID is required for some URLs when an API is called. Therefore, you need to obtain a project ID in advance. Two methods are available:

- **Obtain the Project ID by Calling an API**
- **Obtain the Project ID from the Console**

Obtain the Project ID by Calling an API

You can obtain a project ID by calling the API used to **query projects based on specified criteria**.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. {Endpoint} is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

The following is an example response. The value of **id** is the project ID.

```
{
    "projects": [
        {
            "domain_id": "65ewtrgaggshhk1223245sghjlse684b",
            "is_domain": false,
            "parent_id": "65ewtrgaggshhk1223245sghjlse684b",
            "name": "project_name",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4adasfjljaaaakla12334jklga9sasfg"
            },
            "id": "a4adasfjljaaaakla12334jklga9sasfg",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

Obtain a Project ID from the Console

To obtain a project ID from the console, perform the following operations:

1. Log in to the management console.
2. Click the username and select **My Credentials** from the drop-down list.
   On the **API Credentials** page, view the project ID in the project list.

Figure A-1 Viewing the project ID